VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Audit bezpečnosti informací podle normy ISO/IEC 27001:2005

Information Security Audit according to Standard ISO/IEC 27001:2005

Student: Bc. Jiřina Petříková

Vedoucí práce: Ing. Martin Drastich, Ph.D.

Ostrava 2010

„Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracovala samostatně.“

30. dubna 2010 ……

Na tomto místě bych ráda poděkovala vedoucímu práce, panu Ing. Martinu Drastichovi, Ph.D., za jeho cenné rady a připomínky. Dále bych ráda poděkovala panu Ing. Jaroslavu Doležalovi za poskytnutí literatury a užitečných rad, které mi pomohly k dokončení práce.

Obsah:

Úvod

Bezpečnost informací je pojem, který je znám téměř každé firmě. Není však jednoduché představit si komplexnost problému, který se pod tímto pojmem skrývá.

Jeho hlavní podstatou je ochrana informačních aktiv společnosti neboli dat, která mají pro danou organizaci hodnotu. Cena informací neustále roste a s tímto faktem je spojen i zvyšující se počet útoků na informační systémy, krádeží dat a sabotáží. Většina firem je schopna zabezpečit svůj informační systém pomocí hesel, firewallů nebo nastavením oprávnění ke složkám či souborům. Je však toto zabezpečení dostačující? Bez potřebných zkušeností z oblasti bezpečnosti nemá firma přehled o všech hrozbách, které činí její data zranitelnými a z tohoto důvodu je neumí dostatečně chránit. Vznikly proto určité návody (standardy), ve kterých se odráží zkušenosti s nejčastějšími bezpečnostními hrozbami a které pomáhají předcházet úniku, poškození či ztrátě dat firmy.

Příčiny vedoucí k potřebě ochrany dat mohou být různé. Jedná se například o požadavky zákonů, smluvní ujednání, místní zvyklosti nebo ochranu tzv. know-how dané firmy.

Potřeba ochrany informací je u každé firmy individuální. Vyšší míru zabezpečení vyžadují organizace s velkým počtem zaměstnanců nebo společnosti pracující s citlivými daty. Naopak malé firmy s nízkou hodnotou informačních aktiv si mohou dovolit bezpečnostní opatření, která jsou finančně méně náročná.

Jako metodiku pro svou práci jsem si zvolila normu ISO/IEC 27001, která je mezinárodně uznávaným standardem pro hodnocení bezpečnosti informací a lze ji užít u všech typů organizací, bez ohledu na jejich velikost, či obor činností. Tato norma je hojně využívána i v České republice a to při zavádění systému řízení bezpečnosti, který je důležitým krokem k optimální ochraně informačních aktiv společnosti.

Zákazník si nepřál, aby jméno společnosti bylo použito v této práci. Některé údaje jsou proto upraveny a o firmě budu dále psát jako o Výrobním podniku a.s.

První část mé diplomové práce se bude zabývat stručným seznámením s pojmem bezpečnost informací, dále bude zaměřena na podrobnou charakteristiku normy ISO/IEC 27001 a s ní související systém řízení. Na závěr této části bude také krátce popsán audit bezpečnosti informací a základy psychologie a komunikace, které jsou zapotřebí pro vykonávání činnosti auditora IS.

Druhá část se bude věnovat přípravě auditu podle dané normy. V této části bude sestaven plán auditu a bude upřesněn způsob hodnocení, který bude při auditu použit.

Ve třetí části bude proveden audit bezpečnosti informací v dané firmě. Každý cíl normy bude zhodnocen podle míry plnění jednotlivých bezpečnostních opatření a v případě zjištěných pochybení vůči pravidlům normy bude navrhnuto jejich řešení.

Cílem diplomové práce je zhodnotit systém managementu bezpečnosti informací dané firmy, upozornit na možné zranitelnosti v informačním systému a poskytnout návrh na nápravu zjištěných nedostatků.

1 Teoretická východiska auditu bezpečnosti informací

1.1 Bezpečnost informací

1.1.1 Vysvětlení pojmu

Jedna z nejcennějších aktiv, která mají organizace k dispozici, jsou know-how a obchodní tajemství v podobě informací. Díky tomu se adekvátní informační bezpečnost stává nejen tržní výhodou, ale i nutností umožňující obstát v konkurenčním prostředí. Dosahování stanovených podnikatelských cílů i plnění legislativních úloh je ve velké míře závislé na spolehlivém a efektivním zpracovávání informací.

Informace mohou existovat v nejrůznějších podobách. Mohou být vytištěny nebo napsány na papíře, uloženy v elektronické podobě, posílány poštou, zachyceny na film nebo vyřčeny při konverzaci.

Se vzrůstající propojeností prostředí jednotlivých organizací je potřeba ochrany informací stále více aktuální. Počet různých hrozeb a útoků se neustále zvyšuje a z tohoto důvodu je třeba věnovat pozornost zabezpečení důležitých aktiv organizace. Bezpečnost informací se snaží těmto incidentům zamezit a zajišťuje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout použitím soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury a také programových a hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována, přezkoumávána a zlepšována proto, aby bylo dosaženo specifických bezpečnostních cílů organizace a to v souladu s ostatními řídícími procesy.

1.1.2 Důvody pro řešení informační bezpečnosti

Informace, podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků, ziskovosti, právní shody a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Tyto hrozby se objevují stále častěji, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informací je potřebná z hlediska ochrany kritické infrastruktury a to jak v soukromém, tak ve státním sektoru. V obou sektorech je bezpečnost informací důležitá pro existenci některých služeb, jejichž provoz by bez řízení bezpečnosti představoval velké riziko. Propojení veřejných a privátních sítí a sdílení informačních zdrojů zvyšuje obtížnost řízení přístupu. Trend směřující k distribuovanému zpracování oslabil efektivnost centrální kontroly prováděné specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné. Bezpečnost, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutné pečlivé plánování a rozbor každého detailu. Řízení bezpečnosti informací proto vyžaduje alespoň nějakou spoluúčast všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci majitelů organizace, dodavatelů, třetích stran, zákazníků a dalších externích subjektů. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací. [3]

1.1.3 Hrozby

Aktiva uložená v informačním systému jsou předmětem mnoha typů hrozeb. Hrozba má potenciální schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejich aktiv. Tato škoda se může vyskytnout jako důsledek přímého nebo nepřímého útoku na informační systém. Myšlena jsou například data uložená v rámci informačního systému nebo služby, které systém využívá.

Důsledkem pak je například jejich neautorizované zničení, zpřístupnění, modifikace, deformace a nedostupnost nebo ztráta.

Základní rozdělení hrozeb

Hrozby mají původ buď přírodní (zemětřesení, blesk) nebo lidský (odposlech, chyba uživatele, apod.). Dále hrozby rozlišujeme na náhodné (vymazání souboru) a úmyslné (krádež). Z hlediska bezpečnosti je žádoucí, aby jak náhodné tak úmyslné hrozby byly identifikovány a byla odhadnuta jejich úroveň a pravděpodobnost. [8]

Hrozby mohou ovlivnit specifické části organizace mnoha různými způsoby. Mezi nejčastější patří například narušení serverů a následně i osobních počítačů. Hrozby se mohou také vztahovat k okolnímu prostředí určitého místa, ve kterém systém nebo organizace působí, např. poškození budov vichřicí nebo blesky. Škoda způsobená nežádoucím incidentem může být dočasné povahy nebo může být trvalá, jako je tomu v případě zničení aktiv.

Posouzení hrozeb

Posouzení hrozeb provádíme vždy v závislosti na následujících otázkách:

- ztráta důvěrnosti - může vést například ke ztrátě důvěry zákazníků, právní odpovědnosti, ohrožení osobní bezpečnosti nebo finanční ztrátě;
- ztráta integrity - může vést například k přijetí nesprávných rozhodnutí, rozpadu funkčnosti organizace;
- ztráta dostupnosti - může vést například k neschopnosti vykonávat kritické činnosti organizace;
- ztráta individuální odpovědnosti - může vést například k podvodu, špionáži, krádeži;
- ztráta autentičnosti - může vést například k použití neplatných dat, která vedou k neplatným výsledkům;
- ztráta spolehlivosti - může vést například k nespolehlivým dodavatelům, demotivaci zaměstnanců.

Při stanovení míry hrozeb a typů hrozeb je doporučováno využít standardní dělení, které vychází z předchozího seznamu. To znamená podívat se na každé aktivum z hlediska hrozby a dopadu například ztráty důvěrnosti.

Pro určení nebezpečí, které hrozba pro organizaci představuje, je také vhodné brát v úvahu tzv. následné efekty hrozby. Například výpadek elektrické energie neznamená jen nedostupnost dat, ale může vést při dlouhodobém výpadku k ohrožení činnosti organizace, případně i ohrožení člověka (nemocnice, hasiči, policie). Vždy je třeba promyslet možné dopady hrozeb do nejmenších podrobností. [8]

Nejčastější hrozby

Standardizovaný seznam možných hrozeb pro informační aktiva čítá 46 položek. Následující výčet představuje bezpečnostní incidenty s největším dopadem na informační systémy.

Selhání dodávky energie − Selhání dodávky energie může způsobit problémy z hlediska integrity a následně může způsobit i další poruchy (selhání HW apod.). Selhání dodávky se samozřejmě netýká jen vlastního HW, ale také klimatizace, celého síťového prostředí, zálohování a podobně.

Škodlivý software − Škodlivý software může být použit ke zmaření autentizace a všech souvisejících služeb a bezpečnostních funkcí. Ve svém důsledku může vést ke ztrátě dostupnosti, jestliže jsou např. data nebo soubory zničeny osobou, která získala neautorizovaný přístup pomocí škodlivého programového kódu, nebo vlastním škodlivým programovým kódem.

Selhání hardwaru − Technické poruchy, např. v síti, mohou zničit dostupnost jakékoliv informace, která je uchovávána nebo zpracovávána v této síti. Mezi nejčastější příčiny selhání hardware patří například nedostatečná údržba, nejasné postupy při údržbě HW, nevhodné prostředí umístění HW (vlhkost, prach, výkyvy teploty apod.).

Selhání komunikačních služeb − Chyby a poruchy komunikačních zařízení a služeb ohrožují dostupnost informací přenášených prostřednictvím těchto služeb. Míra ohrožení závisí na příčině chyby nebo poruchy. [8]

1.2 Charakteristika normy ISO/IEC 27001

Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému bezpečnosti informací (*ISMS – Information Security Management System*).

Požadavky této normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků je v případě, že chce organizace dosáhnout souladu s touto normou, nepřijatelné. [2]

Hodnocení rizik

Obecně platí, že výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti. Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky, které by mělo učinit pro předvídání možných hrozeb a pro ochranu informací. Toto hodnocení by mělo být prováděno pravidelně, aby bylo možno včas reagovat na změny v bezpečnostních požadavcích.

V rámci hodnocení rizik by měla být identifikována a kvantifikována rizika a měl by být určen jejich význam s ohledem na cíle organizace. Výstupem z hodnocení rizik by měla být doporučení a priority řízení jednotlivých rizik a priority implementace vybraných opatření na ochranu proti těmto rizikům. Celý proces hodnocení rizik a výběru vhodných opatření může být nutné opakovat pro různé části organizace nebo jednotlivé informační systémy.

Součástí hodnocení rizik by měl být také systematický přístup k odhadu velikosti rizika a proces porovnání odhadnutých rizik se stanovenými kritérii pro určení jejich důležitosti. [3]

1.2.1 Kapitoly

Bezpečnostní politika

Bezpečnostní politika musí odpovídat filozofii organizace. Dotýká se hlavně vybraných aktivit, jako jsou:

- práce se třetími stranami;
- zajištění bezpečnosti informací v rámci pracovních povinností;
- dodržování operačních postupů;
- zabezpečení informačních systémů;
- zabezpečení elektronické pošty;
- zabezpečení přístupových práv;
- omezení přístupů k informacím;
- plánování kontinuity;
- dodržování zákonných požadavků. [5]

Bezpečnostní politika (viz. Příloha 1) stanovuje jasný směr postupu v oblasti bezpečnosti informací. Pro zajištění její neustálé použitelnosti a účinnosti je třeba tuto politiku přezkoumávat v plánovaných intervalech a vždy když nastane významná změna. [3]

Většina firem v době certifikace bezpečnostní politiku má a je schválena vrcholovým vedením organizace. Často ovšem bývá jen formální a nejsou v ní zohledněny výsledky analýzy rizik. Ještě častěji s touto politikou nejsou seznámeni všichni pracovníci organizace.

Organizace bezpečnosti informací

Jedním z důležitých faktorů úspěšné implementace modelu ISMS v organizaci je aktivní podpora vedení organizace, které by mělo jednoznačně přiřadit odpovědnosti za zavedení jednotlivých bezpečnostních opatření. Jasné vyjádření vedení také motivuje zaměstnance ke spolupráci s implementačním týmem a je možné očekávat i konstruktivní návrhy na řešení některých problémů.

U auditovaných firem bývá častým nedostatkem jen formální činnost bezpečnostního fóra. Vlastníci jednotlivých aktiv jsou zpravidla určení, někdy ale chybí vymezení odpovědností za provádění schválených bezpečnostních opatření.

Proces řízení aktiv

Organizace musí být schopna identifikovat svá aktiva a stanovit jejich relativní hodnotu a důležitost. Evidence aktiv pomáhá zajistit udržování efektivní ochrany a může být vyžadována i k jiným účelům, jako je například bezpečnost a ochrana zdraví při práci, pojištění nebo potřeby finančního řízení. [3]

Úroveň ochrany informací by měla být určena na základě požadavků na jejich důvěrnost, integritu, dostupnost a jakýchkoliv dalších požadavků.

Často vyskytující se chybou v této oblasti je neostatečně nebo chybně provedená klasifikace informací. Zpravidla jsou určeny kategorie informací, které ovšem samy o sobě nestačí. Musí být také jasně stanoveno, které informace do které kategorie patří, jakým způsobem mohou být příslušné informace ukládány na přenosná média a jak jsou na elektronických médiích i tištěných výstupech označovány.

Bezpečnost lidských zdrojů

Lidské zdroje jsou nedílnou součástí každé organizace. Bohužel i zde hrozí nebezpečí úniku informací a proto je třeba tuto oblast důsledně kontrolovat. Kontrolní opatření se ovšem netýkají jen současných zaměstnanců organizace, ale i budoucích a minulých.

Při přijímacích pohovorech je třeba klást důraz na prověření daného uchazeče na základě požadavků stanovených organizací s ohledem na hodnotu informací, se kterými by měl uchazeč v případě přijetí pracovat.

Také ukončení pracovního poměru je spjato s bezpečnostními požadavky. Bývalý zaměstnanec má povinnost odevzdat veškeré jemu svěřené prostředky, které jsou majetkem organizace, a musí mu být odejmuta přístupová práva k informacím a prostředkům pro zpracování informací.

Současní zaměstnanci firmy by se měli účastnit bezpečnostních školení z oblasti jejich působnosti, aby byli připraveni na případná bezpečnostní rizika.

V zabezpečení této oblasti nejčastěji dochází k následujícím chybám:

- pracovní smlouvy se zaměstnanci nezohledňují ujednání o bezpečnosti informací;
- není věrohodně prokázáno, že všichni pracovníci prošli odpovídajícím školením z oblasti ISMS;
- i přesto, že je dokumentováno, že všichni zaměstnanci absolvovali příslušná školení, nemají někteří zaměstnanci základní informace o opatřeních, která jsou povinni dodržovat;
- nejsou specifikována disciplinární opatření;
- není dokumentováno, že odcházející zaměstnanec ztratí přístup k důvěrným informacím společnosti. [5]

Fyzická bezpečnost a bezpečnost prostředí

Fyzická bezpečnost si klade za cíl předcházet nepovolenému přístupu do vymezených prostor, předcházet poškození jednotlivých zařízení organizace a zabránit ztrátě, poškození, krádeži nebo kompromitaci dat a tím možnému přerušení činností organizace.

Organizace může věnovat oblasti softwarového zabezpečení nemalé peněžní prostředky, ale pokud je snadný přístup k jednotlivým zařízením, je tu také riziko jejich krádeže a s ním spojené ztráty, kterou organizace jejich zcizením utrpí. Tato oblast se také věnuje zabezpečení dat před jejich znehodnocením. Může se tak stát nejen prostřednictvím úmyslného poškození, ale také díky přírodním katastrofám, nebo uchováváním dat v nevhodném prostředí.

Většina firem nemívá problém s dokumentováním a zpravidla ani s implementací opatření, která se týkají tohoto článku normy. Přijatá opatření jsou závislá na výsledcích analýzy rizik. Nejčastějšími nedostatky jsou:

- v dokumentaci chybí popis oblastí, které mají být chráněny;
- pravidla pro přístup pracovníků jsou příliš přísná a v praxi se pak nedodržují;
- není kontrolována funkčnost náhradních zdrojů elektrické energie, chybí pravidla pro likvidaci zařízení, která obsahovala klasifikované údaje;
- nejsou stanovena pravidla pro přemisťování majetku;
- není věnována pozornost provádění údržby elektrických zařízení. [5]

Řízení komunikace a řízení provozu

Cílem je zajistit správný a bezpečný provoz prostředků pro zpracování informací. Této oblasti se tedy týká i ochrana informačních aktiv proti škodlivým programům a mobilním kódům.

Programy a prostředky pro zpracování informací jsou zranitelné škodlivými programy, jako jsou například počítačové viry, síťoví červi, trojští koně a logické bomby. Uživatelé by měli být upozorňováni na nebezpečí neschválených a škodlivých programů. Vedoucí zaměstnanci by měli tam, kde je to vhodné, aplikovat zvláštní opatření pro jejich předcházení a detekování a zavést postupy pro odstranění těchto hrozeb. [3]

Zálohování je další podstatnou složkou řízení provozu. Pro tuto činnost by měly být vytvořeny rutinní postupy realizující schválenou politiku zálohování a strategii vytváření záložních kopií dat a testování jejich včasného obnovení.

V této oblasti bývá častým problémem, že se zálohy dat netestují a média se zálohami bývají uložena ve stejné místnosti jako zařízení, z kterých se zálohy provádějí. Tím se zvyšuje pravděpodobnost ztráty těchto dat v případě bezpečnostních incidentů.

Řízení přístupu

Přístup k informacím a prostředkům pro zpracování informací by měl být řízen na základě provozních a bezpečnostních požadavků. Tyto postupy by měly pokrývat všechny fáze životního cyklu přístupu uživatele, od jeho prvotní registrace až po konečné zrušení této registrace v momentě, kdy daný uživatel přístup k informačním systémům a službám již dále nepotřebuje. Patří sem také správa hesel k jednotlivým účtům a volba jejich vhodné struktury pro zajištění jejich kvality.

Častým nedostatkem, se kterým se auditoři setkávají, je nedodržování politiky čistého stolu a prázdné obrazovky. V organizacích, ve kterých mají uživatelé povinnost měnit svá hesla častěji, je možné se setkat s hesly poznamenanými přímo v blízkosti firemního počítače, popřípadě je jejich heslo z dostupných materiálů snadno rozluštitelné. Tento fakt může vést k vážným bezpečnostním incidentům, které mohou ohrozit celou organizaci.

Sběr dat, vývoj a údržba informačních systémů

Tato oblast se snaží zajistit, aby se bezpečnost stala neoddělitelnou součástí informačních systémů. To zahrnuje provozní systémy, infrastrukturu, interní aplikace organizace, zakoupené produkty, služby a uživatelsky vyvinuté aplikace. Návrh informačního systému na podporu procesů organizace může být z hlediska bezpečnosti kritický. Bezpečnostní požadavky by měly být stanoveny a odsouhlaseny ještě před zahájením vývoje informačního systému. [3]

Nejčastějšími nedostatky při plnění této kapitoly jsou:

- při formulaci zadání nově vyvíjených aplikací nejsou zohledněny požadavky na zajištění bezpečnosti informací;
- nejsou stanovena pravidla pro kontrolu správnosti vstupních dat do aplikací;
- pracovníci neumí pracovat s kryptografickými prostředky, které mají v popisu činnosti předepsány;
- změny a opravy aplikačních programů jsou prováděny bez náležitého schválení a testování. [5]

Řízení incidentů v oblasti bezpečnosti informací

V tomto článku normy se doporučuje užití formálních postupů pro hlášení bezpečnostních událostí. Všichni zaměstnanci by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a potencionální rizika by měli zaměstnanci ihned hlásit na určené místo. Informace získané při vyhodnocování bezpečnostních incidentů by měly být využity pro identifikaci opakujících se incidentů, aby bylo možné naučit se těmto incidentům předcházet.

Firmy často podceňují zaznamenávání bezpečnostních incidentů a také jejich klasifikaci. Bez těchto záznamů je ovšem těžké provést analýzu daných incidentů a zavést opatření k jejich nápravě.

Řízení kontinuity činností organizace

Hlavní podstatou této oblasti je bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činností.

Pro minimalizaci následků ze ztráty informačních aktiv na přijatelnou úroveň by měl být zaveden proces řízení kontinuity činností organizace a to za pomoci preventivních a zotavovacích opatření. Tento proces by měl identifikovat kritické činnosti organizace a začlenit požadavky řízení bezpečnosti informací s ohledem na požadavky provozní, personální, dopravní a materiální.

Důsledky pohrom, bezpečnostních chyb a přerušení služeb by měly být identifikovány v rámci analýzy dopadů. Pro zajištění obnovy klíčových činností organizace v požadovaných lhůtách je vhodné připravit a implementovat plány kontinuity. Bezpečnost informací by se měla stát nedílnou součástí procesu řízení kontinuity činností a dalších řídících procesů v rámci organizace.

Řízení kontinuity činností organizace by mělo zahrnovat opatření k identifikaci a minimalizaci rizik, omezovat důsledky škodlivých incidentů a zajistit včasnou dostupnost informací potřebných pro obnovení nezbytných činností. [3]

Častým nedostatkem v této oblasti je, že plány kontinuity v organizaci nejsou vůbec vypracovány nebo není otestována jejich funkčnost.

Soulad s požadavky

Pro každý systém by měly být jednoznačně určeny, dokumentovány a udržovány veškeré relevantní zákonné a smluvní požadavky a způsob, jakým je organizace dodržuje. V souladu s těmito požadavky je třeba chránit důležité záznamy organizace proti ztrátě, zničení a padělání.

Častým problémem bývá, že nejsou stanoveny zákony, normy a vyhlášky, kterými se musí zaměstnanci řídit nebo nejsou jejich texty v organizaci k dispozici.

1.2.2 Systém řízení informační bezpečnosti

ISMS je systém řízení a jako takový poskytuje rámec pro efektivnější a přehlednější řízení bezpečnostních procesů v každé organizaci. Sám o sobě nezaručí vyšší nebo „dokonalou" bezpečnost, poskytuje však nástroje, které umožňují vědomě rozhodovat o bezpečnostních problémech a rizikách a vynakládat prostředky do této oblasti efektivně. Cílem ISMS není dosáhnout „bezpečného" informačního systému, ale trvale udržovat bezpečnost informací na takové úrovni, která odpovídá potřebám a požadavkům organizace za vynaložení přiměřených nákladů, a umožnit neustálé transparentní zlepšování se v této oblasti. V tomto smyslu je třeba chápat i certifikáty ISMS podle ISO/IEC 27001 vydané akreditovanými certifikačními organizacemi. Takovýto certifikát nepotvrzuje, že organizace má bezpečný informační systém, ale že proces vybudování, provozu, monitorování a zlepšování informační bezpečnosti je vhodným způsobem řízený.

Model PDCA

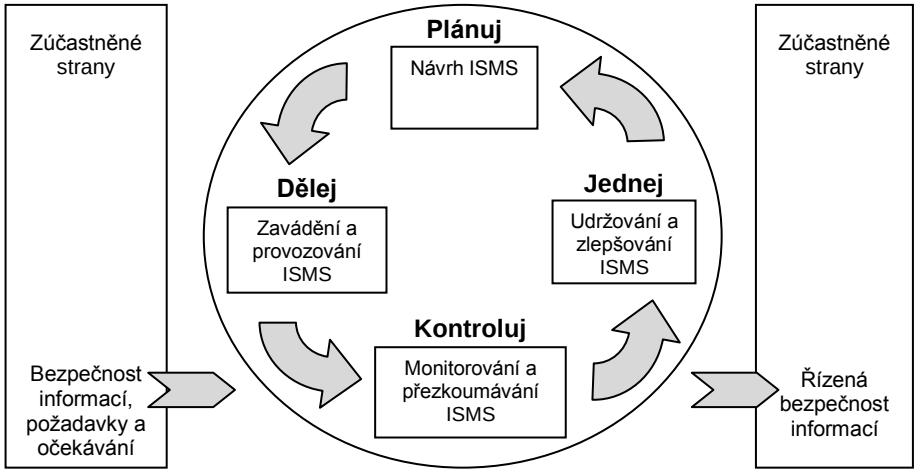
ISMS je založený na soustavném opakováni cyklu "Plánuj-Dělej-Kontroluj-Jednej" (*PDCA – Plan-Do-Check-Act*). Zavedení ISMS znamená definování všech potřebných procesů a první dokončení tohoto cyklu. Konkrétní míra formalizace závisí na velikosti organizace a na stylu jejího řízení.

Plánuj – Plánování představuje základ budování systému řízení informační bezpečnosti. Je stanoven rozsah systému řízení bezpečnosti, je definována bezpečnostní politika, je navrhnuto řízení rizik včetně jejich vyhodnocení a jsou vybrána opatření pro snížení rizik.

Dělej – Fáze „Dělej" zahrnuje zavedení a využívání bezpečnostních opatření, procesů a postupů, včetně monitorování jejich účinnosti.

Kontroluj – V této fázi je posouzena funkčnost a efektivnost procesů a opatření, jsou vykonány interní audity, přehodnocena rizika a je přezkoumán systém řízení bezpečnosti informací.

Jednej – Na základě výsledků předcházející fáze jsou vykonána nápravná a preventivní opatření.



Obr. 1.1 Princip PDCA v ISMS

Podmínky zavedení ISMS

Při budování ISMS je nutné splnit některé předpoklady, bez kterých je zavedení a fungování systému velmi těžké, případně jeho implementace nepřinese očekávaný efekt.

Základním předpokladem pro vybudování ISMS je jasně vyjádřená podpora vedení organizace. Tento požadavek vyplývá přímo z normy ISO/IEC 27001, která vyžaduje, aby bezpečnostní politika ISMS obsahovala jasný závazek vedení v souvislosti s podporou informační bezpečnosti. Kromě toho definuje tato norma další povinnosti vedení organizace. Jedná se hlavně o:

- vytvoření bezpečnostní politiky;
- zabezpečení zpracování bezpečnostních cílů a plánů;
- vytvoření rolí a přidělení zodpovědností;
- poskytnutí dostatečných zdrojů;
- rozhodnutí o akceptovatelné úrovni rizika;
- vykonávání přezkoumání ISMS managementem.

Další podmínkou vybudování ISMS je vyčlenění dostatečných personálních, časových a finančních zdrojů pro jednotlivé etapy celého procesu. Jejich množství závisí na rozsahu systému, charakteru organizace, úrovně už implementovaných bezpečnostních opatření, využití externích konzultačních služeb a podobně. Zavedení systému však vždy klade zvýšené nároky na interní pracovníky organizace a už v době plánování prací je vhodné s nimi počítat.

Při zavádění informační bezpečnosti většinou dochází ke změnám pracovních postupů, kterými se řídí zaměstnanci na různých úrovních řízení. Součástí zavádění ISMS proto musí být i adekvátní vzdělávací program, jehož cílem je přiměřeně informovat a vzdělávat všechny relevantní zaměstnance. Pro každou cílovou skupinu je potřebné zvolit přiměřené komunikační prostředky, což zabezpečí lepší pochopení a motivaci při implementaci opatření.

Zavádění ISMS se v souladu s normou ISO/IEC 27001 realizuje v následujících etapách:

- návrh ISMS;
- zavedení a provoz ISMS;
- monitorování a přezkoumávání ISMS;
- udržování a zlepšování ISMS.

1.3 Audit IS

1.3.1 Základní pojmy

Audit *(audit)*
systematický, nezávislý a dokumentovaný proces získávání důkazů z auditu a jeho objektivního hodnocení s cílem stanovit rozsah splnění kritérií auditu [ISO 19011:2002]

Plán auditu *(audit plan)*
popis činností a uspořádání organizace auditu [ISO 19011:2002]

Předmět auditu *(audit scope)*
velikost a vymezení/ohraničení auditu [ISO 19011:2002]

Kritéria auditu *(audit criteria)*
soubor politik, postupů nebo požadavků [ISO 19011:2002]

Důkaz z auditu *(audit evidence)*
záznamy, konstatování skutečnosti nebo jiné informace, které souvisejí s kritérii auditu a jsou ověřitelné [ISO 19011:2002]

Zjištění z auditu *(audit findings)*
výsledky hodnocení shromážděných důkazů z auditu podle kritérií auditu [ISO 19011:2002]

Závěr z auditu *(audit conclusion)*
výstup z auditu poskytnutý týmem auditorů po zvážení cílů auditu a všech zjištění z auditu [ISO 19011:2002]

Klient auditu *(audit client)*
organizace nebo osoba žádající o audit [ISO 19011:2002]

1.3.2 Podstata certifikace ISMS a její průběh

Po úspěšném nasazení a zprovoznění ISMS by měla následovat jeho certifikace. Certifikace ISMS je nezávislé prověření nasazení a trvalé provozuschopnosti ISMS prostřednictvím auditu třetí stranou (akreditovanou certifikační organizací). Aby byl certifikační audit ISMS hodnověrný a objektivní, vykonávají ho akreditované certifikační společnosti jednotně podle certifikační normy ISO/IEC 27001:2005.

Certifikace ISMS je tedy objektivní ověření už provozovaného systému a zdokumentování shody s požadavky příslušné certifikační normy.

Při auditu se na základě důkazů z auditu zjistí, v jakém rozsahu byla splněna kritéria, která byla pro budovaný systém předem stanovena. Cílem certifikace je veřejné potvrzení systémového přístupu vrcholového managementu organizace k ochraně informačních aktiv a vlastního know-how.

Audit ISMS se vykonává principem náhodné kontroly vybraných prvků ISMS. Při této kontrole probíhá přezkoumání důkazů z auditu, které jsou určeny na základě příslušné normy. Klientem požadované a odůvodněné neuplatňování některého článku normy z rozsahu ISMS, povolené pravidly platnými pro nasazování daného systému řízení, se nazývá výluka.

Rozsah a hranice ISMS definuje předmět auditu. V předmětu auditu se stanoví působnost ve smyslu charakteristik podnikání organizace, aktiv, technologií a lokality. V předmětu auditu se taky podchytí základ zdůvodnění výluk z rozsahu působnosti ISMS. Samotný audit vykonává osoba s prokázanými osobními vlastnostmi a kompetencí provádět profesionální a nezávislé přezkoumání systému řízení bezpečnosti.

Postup certifikace

Certifikace začíná první fází přípravy na audit, která slouží na prověření toho, do jaké míry je vykonání certifikačního auditu možné. Obvykle spočívá ve vyhodnocení informativního dotazníku k certifikaci, který poskytla na vyplnění certifikační společnost klientovi v rámci přípravy na certifikaci. Na základě přezkoumání poskytnutých informací o rozsahu a cílech ISMS, lokalitách jeho nasazení a působnosti organizace, certifikační společnost zhodnotí svoji kompetentnost k certifikaci a vypracuje nabídku na certifikační audit.

V rámci druhé fáze se musí ověřit a zdokumentovat způsobilost ISMS na certifikaci. To je vyřešeno formou prověrky ISMS, kterou provádí auditor z hlediska souladu systému s normou.

V úvodu auditor zjišťuje, jestli jsou k dispozici povinné dokumenty ISMS a vykoná jejich přezkoumání. Dále je třeba zjistit, jestli je ISMS již zprovozněný, zda už byl podroben internímu auditu a přezkoumán vedením. Na závěr druhé fáze musí auditor zkontrolovat dokumentaci ISMS, zhodnotit vhodnost a dostatečnost zdrojů ISMS pro třetí fázi a svoje zjištění zdokumentovat. V této dokumentaci popíše problémy, které by mohly ve třetí fázi auditu vést k neshodám a doporučí klientovi změny a doplnění systému potřebné před realizací třetí fáze.

Cílem třetí fáze je zhodnotit zavedení a efektivnost ISMS. Jde o samotný certifikační audit na místě, který se dělí na následující kroky:

- plánování auditu;
- vykonání auditu;
- následný audit (např. po odstranění systémové neshody);
- zhodnocení závěrů auditu.

Na základě přezkoumání ISMS na konci druhé fáze sestaví auditor plán auditu, který odsouhlasí s klientem. Audit na místě začíná úvodním pohovorem s vedením organizace. Odsouhlasí se proveditelnost navrhovaného plánu auditu, předmět auditu, utajení informací získaných při auditu, stanoví se průvodci auditora a další důležité záležitosti. Auditorem připravený kontrolní seznam otázek slouží během auditu jako pracovní pomůcka.

V případě zjištění systémové neshody během auditu rozhoduje auditor o případném přerušení výkonu auditu na místě. Na základě získaných informací shromáždí vedoucí auditor důkazy o shodě a na jejich základě vypracuje dokumentaci z auditu. Současně písemně vypracuje zprávy o neshodách a doporučeních, se kterými v rámci závěrečného rokování obeznámí vedení organizace – klienta auditu. Zodpovídá za vypracování zprávy z auditu, odsouhlasení jejího obsahu a její odevzdání certifikačnímu orgánu. V případě zjištění systémových neshod rozhodne auditor o čase a rozsahu vykonání následného auditu. K uvolnění dokumentace z auditu a k udělení certifikátu může dojít jen tehdy, když jsou odstraněny všechny systémové neshody a jejich odstranění bylo vhodnou formou zdokumentováno a auditorem potvrzeno.

Ve čtvrté fázi se rozhodne o udělení certifikátu. Certifikát ISMS vydává certifikační orgán po přezkoumání dokumentace z auditu, kterou vypracoval a zaslal na schválení auditor. Tyto informace musí obsahovat zprávu z auditu, komentáře k neshodám, vyhodnocení nápravných činností klienta, odsouhlasení informací, které klient poskytl certifikačnímu orgánu a doporučení auditora na udělení certifikátu s případnými podmínkami. Certifikační orgán rozhodne o certifikaci ISMS na základě závěrů z auditu a dalších zjištěných informací souvisejících s klientem.

Po úspěšném auditu udělí certifikační společnost na provozovaný ISMS certifikát. Certifikát je objektivním potvrzením toho, že proces vybudování, provozu, monitorování a zlepšování informační bezpečnosti je v organizaci vhodně řízen a že management organizace svým přístupem k provozu ISMS zaručuje trvalé zlepšování informační bezpečnosti organizace.

Certifikát ISMS se vydává na období tří let, během kterých se musí minimálně jednou ročně vykonávat kontrolní audit provozovaného ISMS. Tento audit je prováděn certifikační společností za účelem průběžné kontroly. Kontrolní audit nemusí nevyhnutelně zahrnovat celý systém, musí však vždy zahrnovat některé povinné oblasti jako jsou interní audity, splnění povinností managementu, kontrola odstranění neshod z předcházejícího auditu, vyřizování stížností na ISMS, přezkoumání změn, bezpečnostních událostí a opatření proti rizikům. Musí také prověřit efektivnost ISMS vzhledem k záměrům managementu, politiku informační bezpečnosti a cíle klíčových činností organizace. Kompetentní pracovníci certifikačního orgánu tak pravidelně při kontrolních auditech prověřují, jestli klient i nadále splňuje požadavky normy. Udržování certifikace vychází z objektivního ověřování funkčnosti certifikovaného ISMS, ale i z trendů jeho trvalého zlepšování.

Před uplynutím tříletého cyklu platnosti certifikátu se naplánuje a uskuteční recertifikační audit, při kterém se opět prověří shoda se všemi požadavky certifikační normy s přihlédnutím k interním a externím změnám v organizaci. Tento audit zahrnuje přezkoumání výkonnosti ISMS, jeho trvalou aplikovatelnost na rozsah certifikace a splnění závěrů z předcházejících kontrolních auditů. Druhá fáze se při recertifikaci opětovně vykonává tehdy, pokud došlo k významným změnám u klienta nebo v právních a regulačních požadavcích na ISMS.

1.3.3 Základy psychologie a komunikace pro auditory IS

Práce auditora má jasná pravidla tvořená požadavky zákazníka a stanovenými závaznými normami. Auditor by měl především dobře zvládat techniky a problematiku auditu a současně umět komunikovat s protistranami v auditované organizaci. Z toho pohledu to znamená, že ve funkci auditora se skrývají minimálně dvě role – jednak role kontrolní a jednak role urychlovače změn v auditované organizaci. Vykonávání těchto rolí s různými činnostmi s sebou nese také rozdílné kompetence a zdroje.

V roli kontrolní je přezkoušet, zda byl splněn požadavek souladu s příslušnou normou. V roli urychlovače změny jde především o to, dovést systémem otázek komunikačního partnera z auditované organizace k sebereflexi v prováděných aktivitách.

Předpokladem dobrého výkonu funkce auditora je především kultivovat v sobě následující postoje:

- nedělat unáhlená rozhodnutí – tento přístup vede k důslednějšímu pochopení skutečné situace a pomáhá vést rozhovor s vysokou vypovídací hodnotou;
- mít respekt vůči výrokům druhých;
- uvědomovat si, že dotazovaní mají zpravidla dle svého úhlu pohledu pravdu – umění je dotazovat se tak, aby si uvědomili, že to není pravda objektivní;
- učit se klást otázky s dostatečným prostorem pro odpovědi protistrany;
- osobní mínění není stěžejní.

Auditor by měl také velmi dobře ovládat neverbální komunikaci. Do neverbálních sdělení zahrnujeme vše, co obsahuje jakékoli mimoslovní výrazové prostředky např. gestikulaci, mimiku, celkové držení těla a v neposlední řadě i mezilidskou vzdálenost. Tato komunikace je často účinnější než slova. Pozorný a citlivý pozorovatel dokáže tuto řeč těla číst. Pří komunikaci je proto důležité, aby slova a mimoslovní vyjádření byly v souladu.

Pro vytvoření příznivých podmínek pro vedení kvalitního rozhovoru by se měl auditor řídit následujícími fázemi mezilidské komunikace:

1. navázání kontaktu – pozdrav, vytvoření příznivého dojmu;
2. otevírací fáze – zahájení rozhovoru s odpovědnými pracovníky organizace;
    a. vymezení cíle a účelu auditu;
    b. vymezení časového plánu;
    c. vymezení pravidel komunikace.
3. informační fáze – využití komunikačních technik (dotazování, naslouchání) ke sběru informací, konkrétních hodnot, dat a faktů;
4. argumentační fáze – diskuse o různých stanoviskách. V této fázi se osvědčuje využití především otevřených otázek;
5. fáze objasnění – vytváří se ucelená struktura reálné situace, předpoklady se stávají měřitelnými. [7]

2 Návrh struktury zpracování auditu

2.1 Cíle přehledového auditu

Cílem auditu je dát odpověď na otázku, které procesy je potřeba u organizace řešit. Přehledový bezpečnostní audit organizace je velmi efektivním nástrojem, který rychle poskytne informace o mezerách v řízení bezpečnosti a chybějících bezpečnostních opatřeních.

2.2 Plán auditu

Audit je třeba naplánovat tak, aby byl efektivní a úsporný. Neefektivnost může způsobit chyby v průběhu auditu nebo může udělat audit finančně náročnější. Proto se před auditem sestavuje jeho plán na základě znalosti podnikatelské činnosti organizace. Plán auditu určuje časové rozvržení činností v průběhu auditu a zároveň usnadňuje jejich koordinaci. Tento plán by měl být zároveň dostatečně flexibilní pro případ, že by ho bylo nutné v průběhu auditu měnit.

Plán interního auditu zpracovává auditor ve spolupráci s vedením auditované firmy. Měl by být minimálně týden před termínem auditu předložen vedení společnosti, které má povinnost ho přezkoumat a vyjádřit se k němu. Na závěr musí být plán auditu schválen jak ze strany auditora, tak ze strany auditovaných.

Plán auditu by měl obsahovat cíle auditu, harmonogram prověření jednotlivých článků normy a určení odpovědných pracovníků, kteří musí být přítomni.

Pro přehledový audit společnosti Výrobní podnik a.s. jsem vypracovala následující plán, který byl poté ověřen a schválen vedením společnosti. Termín pro vykonání auditu byl stanoven na 8. 2. 2010.

Plán auditu pro firmu Výrobní podnik a.s.

Cíle auditu:

1. Získání obecného přehledu o stavu a úrovni řízení bezpečnosti u organizace.
2. Nalezení problematických míst v ISMS a návrh jejich řešení.

Čas	Článek normy	Odpovědná osoba
9:00 – 10:00	A.5 Bezpečnostní politika A.6 Organizace bezpečnosti informací	Jednatel
10:00 - 11:30	A.7 Řízení aktiv A.9 Fyzická bezpečnost a bezpečnost prostředí A.10 Řízení komunikace a řízení provozu	Manažer bezpečnosti
11:30 – 12:30	A.8 Bezpečnost lidských zdrojů	Personalista
12:30 – 13:30	A.11 Řízení přístupu A.12 Údržba IS	Administrátor
13:30 – 15:00	A.12 Sběr dat, vývoj IS A.13 Řízení incidentů v oblasti bezpečnosti informací A.14 Řízení kontinuity činností organizace	Manažer bezpečnosti
15:00 – 16: 00	A.14 Řízení kontinuity činností organizace A.15 Soulad s požadavky	Jednatel

Tab. 2.1 Plán auditu

Vlastní audit bude proveden formou interview se zástupci organizace, na kterých se bude zjišťovat stav realizace jednotlivých opatření.

2.3 Hodnocení auditu

Ústní hodnocení jednotlivých opatření nemusí být pro organizaci dostatečně vypovídající. Před auditem je proto vhodné sestavit číselný systém hodnocení, který dovoluje firmě lépe si uvědomit, v jaké míře jsou splněny jednotlivé požadavky hodnotící normy, a poskytuje jasný přehled o zásadních nedostatcích, které se v ISMS vyskytují.

V průběhu auditu bude tedy každé opatření prodiskutováno a bude mu přiděleno hodnocení, vyjadřující míru souladu s požadavky standardu v rozsahu od 0 (opatření není vůbec naplněno, nebo chybí) do 100 (opatření je odpovídajícím způsobem naplněno).

Pro přehled o míře souladu s požadavky normy jsem zvolila systém hodnocení znázorněný v následující tabulce (viz. Tab. 2.2).

Míra plnění	Hodnocení
Opatření není zavedeno	0
Předmět otázky nebyl splněn; byla zavedena jen základní opatření, která jsou nevyhovující	20
Předmět otázky byl částečně splněn, ale podstatná část opatření není zavedena	40
Předmět otázky byl z větší části splněn	60
Předmět otázky byl převážně splněn; odchylka od hodnotící normy je velmi malá	80
Opatření je zavedeno	100

Tab. 2.2 Hodnocení jednotlivých opatření

Po provedení vlastního auditu budou hodnoty jednotlivých opatření dosazeny do vzorce (2.3), kdy se sečtou míry plnění všech opatření daného cíle řízení bezpečnosti a tato suma pak bude vydělena počtem opatření náležících tomuto cíli. Tento výpočet bude proveden postupně u všech cílů ISMS. Výsledné hodnoty jednotlivých cílů pak budou dosazeny do vzorce (2.4), čímž bude vypočtena celková míra plnění systému řízení bezpečnosti dané organizace.

$$MP_C^{1} = \frac{\text{Součet hodnocení jednotlivých opatření daného cíle}}{\text{Počet opatření daného cíle}} \quad [\%] \qquad (2.3)$$

$$MP_{ISMS}^{2} = \frac{\text{Součet měr plnění všech cílů ISMS}}{\text{Počet cílů v ISMS}} \quad [\%] \qquad (2.4)$$

[1] MP_C je míra plnění daného cíle
[2] MP_{ISMS} je míra plnění systému řízení bezpečnosti informací

3 Provedení auditu ve firmě

3.1 Vlastní audit

Při auditu jsem postupovala v souladu s normou ISO/IEC 27001:2005. Tuto normu tvoří 11 oblastí bezpečnosti, 39 cílů a 133 bezpečnostních opatření. Systém číslování, který jsem při auditu použila, odpovídá číselnému značení v samotném standardu.

Oblasti bezpečnosti jsou uvedeny v nadpisu první úrovně, v nadpisu druhé úrovně jsou uvedeny cíle, které patří do dané oblasti a na třetí úrovni jsou uvedena příslušná bezpečnostní opatření. U každého opatření je pak zjištěn stav jeho realizace a je mu přiděleno hodnocení podle souladu s danou normou. Číselné hodnocení těchto opatření je obsaženo v tabulce (viz. Příloha 2).

Požadavky standardu jsou v jednotlivých statích psány kurzívou, aby byl odlišen text standardu od vlastního hodnocení.

A.5 Bezpečnostní politika

A.5.1 Bezpečnostní politika informací

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a směrnicemi.

Společnost má bezpečnostní politiku informací pod názvem „Základní bezpečnostní cíle a strategie a organizace bezpečnostní politiky informačního systému“.

A.5.1.1 Dokument bezpečnostní politiky informací

Dokument bezpečnostní politiky informací musí být schválen vedením organizace, publikován a dán na vědomí všem zaměstnancům a relevantním externím stranám.

Už jen pouhý fakt, že společnost takový dokument má, je významným přínosem pro řízení bezpečnosti. Dokument bezpečnostní politiky ale nepokrývá svým rozsahem potřebné oblasti. Dokument nebyl vytvořen na základě bezpečnostní analýzy, takže jednotlivá opatření nelze zdůvodnit.

Dokument nebyl schválen vedením společnosti, takže jeho validita je sporná.

A.5.1.2 Přezkoumání bezpečnostní politiky informací

Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti musí být bezpečnostní politika informací přezkoumávána v plánovaných intervalech a vždy když nastane významná změna.

Přezkoumání a aktualizace bezpečnostní politiky není prováděno, o čemž v politice svědčí odkazy na zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a změně některých zákonů, který byl v plném rozsahu nahrazen zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Řídit bezpečnost informací v organizaci.

A.6.1.1 Závazek vedení směrem k bezpečnosti informací

Vedení organizace musí stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace. Mělo by demonstrovat svůj závazek a jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací.

V bezpečnostní politice jsou sice vymezeny základní role (Bezpečnostní výbor), není ovšem složen ze členů vrcholového managementu a jeho podpora prosazování bezpečnosti je pouze deklarativní. Z tříčlenného výboru je manažer informační a datové bezpečnosti a manažer IT prezentován touž osobou.

Vedení společnosti nevyhodnocuje pravidelně stav bezpečnosti a nevede o tom záznamy, nemá plán poskytování zdrojů pro bezpečnost atd.

A.6.1.2 Koordinace bezpečnosti informací

Činnosti v oblasti bezpečnosti informací musí být koordinovány prostřednictvím zástupců různých útvarů z celé organizace s odpovídajícími rolemi a pracovním zařazením.

V rámci společnosti je toto řešeno jen částečně. Nepromítá se stav bezpečnosti do dokumentace − neprobíhá kontrola a vyhodnocení a následné promítnutí změn do dokumentace.

A.6.1.3 Přidělení odpovědností v oblasti bezpečnosti informací

Musí být jasně definovány odpovědnosti v oblasti bezpečnosti informací.

Odpovědnosti za ochranu aktiv jsou jasně definovány.

A.6.1.4 Schvalovací proces prostředků pro zpracování informací

Musí být stanoven a zaveden postup schvalování (vedoucími zaměstnanci) nových prostředků pro zpracování informací.

Nasazení nových prostředků schvaluje investiční komise. Postupy před nasazením nové techniky nejsou. Pouze v systému SAP je testovací systém.

A.6.1.5 Dohody o ochraně důvěrných informací

Musí být určeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.

Dohody na ochranu obchodního tajemství podle §17 Obchodního zákoníku jsou uzavírány. Nosiče s informacemi charakteru obchodního tajemství ale nejsou označeny, takže může v dobré víře dojít k neoprávněnému nakládání s těmito informacemi.

A.6.1.6 Kontakt s orgány veřejné správy

Musí být udržovány přiměřené vztahy s orgány veřejné správy.

Je řešeno v organizačním řádu.

A.6.1.7 Kontakt se zájmovými skupinami

Musí být udržovány přiměřené vztahy se zájmovými skupinami nebo speciálními fóry na bezpečnost a profesními sdruženími.

Je řešeno v organizačním řádu.

A.6.1.8 Nezávislá přezkoumání bezpečnosti informací

Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cíle opatření, jednotlivá opatření, politiky, směrnice a postupy) musí být v pravidelných intervalech (anebo v případě jakékoliv významné změny ve vztahu k bezpečnosti) nezávisle přezkoumávány.

Pravidelné přezkoumávání se neprovádí.

A.6.2 Externí subjekty

Cíl: Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.

A.6.2.1 Identifikace rizik plynoucích z přístupu externích subjektů

Předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací, musí být identifikována rizika a implementována vhodná opatření na jejich pokrytí.

Řeší se nahodile jako neformalizované procedury (dohody na ochranu obchodního tajemství).

Společnost má smlouvu s dodavatelem software o podpoře IS (výrobní systém pro řízení a plánování výroby). Externí zaměstnanci mají smlouvu o ochraně obchodního tajemství.

A.6.2.2 Bezpečnostní požadavky pro přístup klientů

Předtím, než je klientům umožněn přístup k informacím nebo aktivům organizace, musí být identifikované všechny požadavky na bezpečnost

Řeší se nahodile jako neformalizované procedury (dohody na ochranu obchodního tajemství). Pro přístup klientů je používána VPN. Pro povolování přístupu je procedura schvalování přístupu.

A.6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou

Dohody uzavřené s třetími stranami zahrnující přístup, zpracování, sdělování nebo správu informací organizace nebo správu prostředků pro zpracování informací, případně dodávku produktů nebo služeb k zařízení pro zpracování informací, musí pokrývat veškeré relevantní bezpečnostní požadavky.

Řeší se nahodile jako neformalizované procedury (dohody na ochranu obchodního tajemství). Nejsou určeny postupy pro stanovování takovýchto bezpečnostních požadavků.

A.7 Řízení aktiv

A.7.1 Odpovědnost za aktiva

Cíl: Nastavit a udržovat přiměřenou ochranu aktiv organizace.

A.7.1.1 Evidence aktiv

Musí být jasně identifikována všechna aktiva organizace, všechna důležitá aktiva musí být evidována a seznam udržován aktuální.

Seznam aktiv je jen v analýze rizik, informace charakteru obchodního tajemství nejsou evidovány. Společnost nemá přehled, kolik nosičů s informacemi charakteru obchodního tajemství ve společnosti existuje. Hrubý přehled informačních aktiv IT je uveden v analýze rizik.

A.7.1.2 Vlastnictví aktiv

Veškeré informace a aktiva související s prostředky pro zpracování informací musí mít určeného vlastníka.

Princip vlastnictví aktiv ve společnosti není zaveden.

A.7.1.3 Přípustné použití aktiv

Musí být určena, dokumentována a do praxe zavedena pravidla pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.

Řeší směrnice „Informační technologie“.

A.7.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany.

A.7.2.1 Doporučení pro klasifikaci

Informace musí být klasifikovány a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.

Tato problematika není ve společnosti řešena.

A.7.2.2 Označování a nakládání s informacemi

Pro označování informací a zacházení s nimi musí být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.

Tato problematika není ve společnosti řešena.

A.8 Bezpečnost lidských zdrojů

A.8.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

A.8.1.1 Role a odpovědnosti

Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací musí být definovány a dokumentovány v souladu s bezpečnostní politikou organizace.

Na pozice THP jsou předdefinované pracovní náplně, není definováno na dělnické profese. Ochrana informací je součástí smlouvy.

A.8.1.2 Prověřování

Všichni uchazeči o zaměstnání, smluvní a třetí strany musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti a potenciálních rizik.

Tato problematika není ve společnosti řešena.

A.8.1.3 Podmínky výkonu pracovní činnosti

Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami musí obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.

Realizuje se pouze na úrovni závazku ochrany obchodního tajemství, který je podepsán u všech zaměstnanců společnosti. V pracovních smlouvách je závazek dodržovat bezpečnostní normativy společnosti. Problematika na úrovni jednotlivce není řešena se smluvními a třetími stranami.

A.8.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

Problematika je řešena pracovním řádem. Pracovní řád explicitně neřeší problematiku bezpečnosti (pouze bezpečnost práce). V základních povinnostech zaměstnance by se měl výrazněji objevit aspekt ochrany informací a obchodního tajemství.

A.8.2.1 Odpovědnosti vedoucích zaměstnanců

Vedoucí zaměstnanci musí po uživatelích, smluvních a třetích stranách požadovat dodržování bezpečnosti v souladu se zavedenými politikami a postupy.

Odpovědnosti vedoucích zaměstnanců jsou uvedeny v pracovním řádu. Neuvádí se však povinnost znát interní bezpečnostní normativy společnosti a vyžadovat jejich dodržování od podřízených.

A.8.2.2 Informovanost, vzdělávání a školení v oblasti bezpečnosti informací

Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran musí, s ohledem na svou pracovní náplň, absolvovat odpovídající a pravidelně se opakující školení v oblasti bezpečnosti informací, bezpečnostní politiky a směrnic organizace.

Řešeno směrnicí PI-1-09-01, v níž je uvedena povinnost zúčastnit se školení. Školení IT není zahrnuto. Školení bezpečnosti IT není vůbec. Povinnost vedoucího zaměstnance školit bezpečnost je uváděna pouze v souvislosti s bezpečností práce.

A.8.2.3 Disciplinární řízení

Musí existovat formalizované disciplinární řízení vůči zaměstnancům, kteří se dopustili narušení bezpečnosti.

Řešeno pouze sankčním řádem.

A.8.3 Ukončení nebo změna pracovního vztahu

Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

A.8.3.1 Odpovědnosti při ukončení pracovního vztahu

Musí být jasně určeny a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu.

Je stanoveno v pracovním řádu. Organizování ukončení pracovního vztahu je řešeno s důrazem na vrácení materiálu. Mělo by být rozšířeno ještě na opětovné podepsání prohlášení o zachování mlčenlivosti, které odcházejícímu zaměstnanci připomene, že závazek mlčenlivosti trvá i po ukončení pracovního vztahu.

A.8.3.2 Navrácení zapůjčených předmětů

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené předměty, které jsou majetkem organizace.

Realizuje se prostřednictvím „kolečka“ kdy zaměstnanci potvrdí příslušná výdejna vrácení všech zapůjčených předmětů.

A.8.3.3 Odebrání přístupových práv

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna přístupová práva k informacím a prostředkům pro zpracování informací.

Provádí se nahodile, postup není formalizován. Chybí nastavení odpovědností za odebrání přístupových práv.

A.9 Fyzická bezpečnost a bezpečnost prostředí

A.9.1 Zabezpečené oblasti

Cíl: Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

Ve společnosti je kladen patřičný důraz na fyzickou bezpečnost.

A.9.1.1 Fyzický bezpečnostní perimetr

Při ochraně prostor, ve kterých se nachází informace nebo prostředky pro zpracování informací, musí být používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).

Perimetr objektu je řádně zabezpečen. Je nutné udržovat statickou stálost betonového oplocení areálu a zbývající drátěné oplocení nahradit bezpečnostním oplocením. Obvod je pod kontrolou kamerového systému doplňovaného v mimopracovní době obhlídkovou službou. Pro ochranu objektu je používán i pes.

A.9.1.2 Fyzické kontroly vstupu osob

Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.

Kontrola pohybu osob v objektu je řádně zabezpečena systémem přístupových karet a kamerovým systémem.

A.9.1.3 Zabezpečení kanceláří, místností a prostředků

Musí být navrženo a aplikováno fyzické zabezpečení kanceláří, místností a prostředků.

Jsou stanovena pravidla pro pohyb osob a jsou i pravidla pro manipulaci s klíči.

A.9.1.4 Ochrana před hrozbami vnějšku a prostředí

Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami, musí být navrženy a aplikovány prvky fyzické ochrany.

Je řešeno v rámci povinné dokumentace požární ochrany a havarijním plánem společnosti.

A.9.1.5 Práce v zabezpečených oblastech

Pro práci v zabezpečených oblastech musí být navrženy a aplikovány prvky fyzické ochrany.

Jsou stanovena pravidla pro přístup a pohyb osob a jsou i pravidla pro manipulaci s klíči.

A.9.1.6 Veřejný přístup, prostory pro nakládku a vykládku

Prostory pro nakládku a vykládku a další místa, kudy se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolována a pokud možno by měla být izolována od prostředků pro zpracování informací tak, aby se zabránilo neoprávněnému přístupu k nim

Prostory pro nakládku a vykládku materiálu nejsou v závodě určeny a zabezpečeny. Nakládání a vykládání materiálu je možná cesta k neoprávněnému průniku do objektu. Při monitorování pohybu cizích aut po objektu je spoléháno zejména na kamerový systém, což je u závodu, který se zabývá výrobou, nedostatečné.

A.9.2 Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

Bezpečnosti zařízení je věnována pozornost. Ochrana spočívá především v důsledném řízení přístupu osob k aktivům společnosti.

A.9.2.1 Umístění zařízení a jeho ochrana

Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Ochrana spočívá především v důsledném řízení přístupu osob k aktivům společnosti.

A.9.2.2 Podpůrná zařízení

Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Ochrana před výpadky napájení není ve společnosti dostatečně realizována. Rizika výpadků dodávky energie jsou managementu společnosti známa. S budováním náhradního zdroje energie se nepočítá. Náhradní zdroje UPS nepředstavují velkou investici a výrazně by zvýšily spolehlivost chodu informačních systémů společnosti.

A.9.2.3 Bezpečnost kabelových rozvodů

Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem či poškozením.

Ke všem systémům existuje dokumentace, bezpečnost rozvodů je brána v úvahu.

A.9.2.4 Údržba zařízení

Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Zařízení společnosti jsou řádně udržována.

A.9.2.5 Bezpečnost zařízení mimo prostory organizace

Zařízení používané mimo prostory organizace musí být zabezpečeno s přihlédnutím k různým rizikům, která vyplývají z jeho použití mimo organizaci.

Nosiče informací nejsou evidované, přenosné počítače mají personální firewall Kerio, chybí šifrování harddisků a nejsou směrnice, které by stanovovaly, jak chránit zařízení mimo prostory organizace.

A.9.2.6 Bezpečná likvidace nebo opakované použití zařízení

Všechna zařízení obsahující paměťová média musí být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna nebo bezpečně přepsána.

Není řešeno žádnou směrnicí. Závisí pouze na ostražitosti jednotlivých zaměstnanců. V prostorách, kde se vyskytuje obchodní tajemství, jsou instalovány skartovací zařízení.

Bezpečná likvidace médií v IT není řešena.

A.9.2.7 Přemístění majetku

Zařízení, informace nebo programové vybavení nesmí být bez předchozího schválení přemisťováno.

Je řešena přeprava zboží a speciálního materiálu směrnicí „Přeprava zboží a cenností“. Běžné akce, jako stěhování uvnitř nebo vně objektu, nejsou řešeny a závisí jen na rozumném úsudku organizátorů stěhování.

A.10 Řízení komunikací a řízení provozu

A.10.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.

A.10.1.1 Dokumentace provozních postupů

Provozní postupy musí být zdokumentovány a udržovány a musí být dostupné všem uživatelům podle potřeby.

Z provozních postupů v IT je popsáno pouze zálohování.

A.10.1.2 Řízení změn

Změny systémů a prostředků pro zpracování informací musí být řízeny.

Požadavky na změny v IT se zadávají a schvalují prostřednictvím aplikace Intranet. Provádění změn je řízeno pouze u systému SAP.

A.10.1.3 Oddělení povinností

Pro snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení jednotlivých povinností a odpovědností.

Jsou definovány administrátorské a uživatelské účty. Zásada čtyř očí[1] není v IT uplatňována (nejsou stanoveny žádné operace, kde by to bylo vyžadováno).

A.10.1.4 Oddělení vývoje, testování a provozu

Pro snížení rizika neoprávněného přístupu k provoznímu systému anebo jeho změn musí být zajištěno oddělení prostředků vývoje, testování a provozu.

Oddělení vývoje, testování a provozu je realizováno jen u systému SAP a u výrobního systému. Jiné vývojové systémy ve společnosti nejsou.

A.10.2 Řízení dodávek služeb třetích stran

Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávání služeb ve shodě s uzavřenými dohodami.

A.10.2.1 Dodávky služeb

Musí být zajištěno, aby bezpečnostní opatření, definice a úroveň poskytovaných služeb, byly třetí stranou implementovány, provozovány a udržovány ve shodě s uzavřenými dohodami.

Dodávky služeb IT nejsou řešeny prostřednictvím SLA (Service Level Agreement). V servisních smlouvách jsou definovány časy oprav.

[1] „princip čtyř očí“ – kontrolní činnosti, odpovědnosti a povinnosti, které vedou k neomezenému přístupu k systému, nesmí být vykonávány jedinou osobou

A.10.2.2 Monitorování a přezkoumávání služeb třetích stran

Služby, zprávy a záznamy poskytované třetí stranou musí být pravidelně monitorovány a přezkoumávány, audity musí být opakovány v pravidelných intervalech.

Služby monitorovány nejsou. Funkčnost se kontroluje jen v rámci testů, vlastní procedury a pravidla testování nejsou specifikována.

A.10.2.3 Řízení změn služeb poskytovaných třetími stranami

Změny v poskytování služeb, včetně udržování a zlepšování existujících bezpečnostních politik, postupů a bezpečnostních opatření, musí být řízeny s ohledem na kritičnost systémů a procesů organizace, které jsou součástí opakovaného hodnocení rizik.

Přímo tato problematika řešena není, neexistuje ani směrnice. Částečně se tato problematika řeší prostřednictvím hostovaných webových stránek, kde je řešena problematika CRM (Customer Relationship Management).

A.10.3 Plánování a přejímání systémů

Cíl: Minimalizovat riziko selhání systémů.

A.10.3.1 Řízení kapacit

Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.

Výkon informačního systému se pravidelně nesleduje s výjimkou systému SAP, kde se testuje doba odezvy. Hodnocení kapacity informačního systému se provádí jen při plánování změn v IS. Nejsou žádné procedury, které by tuto problematiku řešily.

A.10.3.2 Přejímání systémů

Musí být určena kritéria pro přejímání nových informačních systémů, jejich aktualizaci a zavádění nových verzí a vhodný způsob testování systému v průběhu vývoje a před zavedením do ostrého provozu.

Realizuje se akceptačními protokoly. Požadavky na přejímání systému v bezpečnostní politice nejsou.

A.10.4 Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programového vybavení a dat.

A.10.4.1 Opatření na ochranu proti škodlivým programům

Na ochranu proti škodlivým programům a nepovoleným mobilním kódům musí být implementována opatření na jejich detekci, prevenci a obnovu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.

Antivirová ochrana je řešena kvalitně, produktem e-Trust. Na firewallu běží antivirus Doktor web. Aktualizace vzorových databází antivirů jsou prováděny automaticky. Antivirová ochrana je na dobré úrovni.

A.10.4.2 Opatření na ochranu proti mobilním kódům

Použití povolených mobilních kódů musí být nastaveno v souladu s bezpečnostní politikou, musí být zabráněno spuštění nepovolených mobilních kódů.

Ochrana proti mobilním kódům je řešena na firewallu programem Doktor web. Základní úroveň ochrany je tak zabezpečena. V budoucnosti by bylo vhodné řešit aktivní obsah některých webových stránek a omezení přístupu na nebezpečné webové servery.

A.10.5 Zálohování

Cíl: Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

A.10.5.1 Zálohování informací

Záložní kopie důležitých informací a programového vybavení organizace musí být pořizovány a testovány v pravidelných intervalech.

Zálohování probíhá na páskovou knihovnu, která se nachází mimo objekt IT.

Jednou denně probíhá úplná záloha systémových souborů výrobního systému pro řízení a plánování výroby. Logy SQL se zálohují každé 4 hodiny.

U systému SAP probíhá úplná záloha každé 2 dny, logy systému SAP se zálohují na zálohovacím systému TIVOLI IBM. Testovací systém SAP se zálohuje každé 4 dny. Zálohování je vyřešeno na dobré úrovni.

A.10.6 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.

A.10.6.1 Síťová opatření

Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečnosti informací při přenosu musí být počítačové sítě vhodným způsobem spravovány a kontrolovány.

Bezpečnost sítě vychází z NDS (Novell Directory Services), což je globální distribuovaná replikovatelná databáze uchovávající informace o všech zdrojích sítě. Veškerá práva k síťovým zdrojům jsou definována v seznamech Access Control List, které umožňují řízenou správu přístupu k síťovým zdrojům. Tento prostředek, je-li dobře konfigurován, umožňuje kvalitní řízení bezpečnosti sítě.

A.10.6.2 Bezpečnost síťových služeb

Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu.

Bezpečnost síťových služeb je zabezpečována firewallem, který spravuje externí firma. V případě, kdy společnost má poskytnout přístup „z venku“ jinému subjektu, je přístup umožněn pouze do DMZ (demilitarizované zóny). Začínají se realizovat připojení členů managementu firmy prostřednictvím VPN (virtuální privátní sítě). Takový koncept je bezpečný, důležité je, aby byl řádně zdokumentován.

A.10.7 Bezpečnost při zacházení s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.

A.10.7.1 Správa výměnných počítačových médií

Musí být vytvořeny postupy pro správu výměnných počítačových médií.

Tato problematika není ve společnosti řešena.

A.10.7.2 Likvidace médií

Jestliže jsou média dále provozně neupotřebitelná, musí být bezpečně a spolehlivě zlikvidována v souladu se schválenými postupy.

Tato problematika není ve společnosti řešena.

A.10.7.3 Postupy pro manipulaci s informacemi

Pro zabránění neautorizovanému přístupu nebo zneužití informací musí být stanoveny postupy pro manipulaci s nimi a pro jejich ukládání.

Tato problematika je ve společnosti řešena pouze na úrovni spisového a archivního řádu. Ve společnosti není řešena manipulace s informacemi, ale pouze archivace a skartování.

A.10.7.4 Bezpečnost systémové dokumentace

Systémová dokumentace musí být chráněna proti neoprávněnému přístupu.

Administrátoři drží některá citlivá data týkající se systému odděleně s vyloučením přístupu běžných uživatelů, koncepční řešení systémové dokumentace není vytvořeno.

A.10.8 Výměna informací

Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.

A.10.8.1 Postupy a politiky při výměně informací

Musí být ustaveny a do praxe zavedeny formální politiky, postupy a opatření na ochranu informací při jejich výměně pro všechny typy komunikačních zařízení.

Postupy nejsou řešeny vůbec, některá ochranná opatření vyplývají z dohod o ochraně obchodního tajemství. Řešení této problematiky je nedostatečné.

A.10.8.2 Dohody o výměně informací a programů

Výměna informací a programového vybavení musí být založena na dohodách uzavřených mezi organizací a externími subjekty.

Postupy nejsou řešeny vůbec, některá ochranná opatření vyplývají z dohod o ochraně obchodního tajemství. Řešení této problematiky je nedostatečné.

A.10.8.3 Bezpečnost médií při přepravě

Média obsahující informace musí být během přepravy mimo organizaci chráněna proti neoprávněnému přístupu, zneužití nebo narušení.

Postupy nejsou řešeny vůbec, některá ochranná opatření vyplývají z dohod o ochraně obchodního tajemství. Řešení této problematiky je nedostatečné.

A.10.8.4 Elektronické zasílání zpráv

Elektronicky přenášené informace musí být vhodným způsobem chráněny.

Postupy nejsou řešeny vůbec, některá ochranná opatření vyplývají z dohod o ochraně obchodního tajemství. Řešení této problematiky je nedostatečné.

A.10.8.5 Informační systémy organizace

Na ochranu informací v propojených podnikových informačních systémech musí být vytvořeny a do praxe zavedeny politiky a postupy.

Základní postupy jsou řešeny ve směrnici PI-1-10-04 „Informační technologie“.

A.10.9 Služby elektronického obchodu

Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.

Problematika elektronického obchodu je v počátcích a je řešena outsourcingem.

A.10.10 Monitorováni

Cíl: Detekovat neoprávněné zpracování informací.

A.10.10.1 Pořizování auditních záznamů

Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, musí být pořizovány a uchovány po stanovené období tak, aby se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu.

Na kritických síťových prvcích je podle dokumentu „Bezpečnostní politika síťového provozu IS“ veden záznam běhových událostí (logování). Jedná se zejména o servery, na nichž jsou provozována nehmotná informační aktiva, kritické routery, firewally, nameserver a mailové servery. Požadavek je naplněn.

A.10.10.2 Monitorování používání systému

Musí být stanovena pravidla pro monitorování použití prostředků pro zpracování informací; výsledky těchto monitorování musí být pravidelně přezkoumávány.

Pravidelné vyhodnocování a kontrola využití prostředků IT se neprovádí.

A.10.10.3 Ochrana vytvořených záznamů

Prostředky pro zaznamenávání informací a vytvořené záznamy musí být vhodným způsobem chráněny proti zfalšování a neoprávněnému přístupu.

Záznamy jsou uloženy na médiích s omezeným přístupem jen pro administrátory. Záznamy jsou tak chráněny pouze před běžnými uživateli, nejsou ale chráněny před administrátory.

A.10.10.4 Administrátorský a operátorský deník

Aktivity správce systému a systémového operátora musí být zaznamenávány.

Realizuje se pouze v rámci logování.

A.10.10.5 Záznam selhání

Musí být zaznamenány a analyzovány chyby a přijata příslušná opatření.

Je veden pouze formou žádostí o opravy, které jsou zadávány do aplikace Intranet. Záznamy se nevyhodnocují.

A.10.10.6 Synchronizace hodin

Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostní domény synchronizovány se schváleným zdrojem přesného času.

Společnost má časový server, který je provozován na firewallu.

A.11 Řízení přístupu

A.11.1 Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.

A.11.1.1 Politika řízení přístupu

Musí být vytvořena, zdokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.

Řízení přístupu je řešeno prostřednictvím aplikace Intranet, kdy zaměstnanec požádá o přístup k aktivu a na základě vyjádření nadřízeného se přístup povolí. Udělená povolení nejsou pravidelně přezkoumávána.

A.11.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.

A.11.2.1 Registrace uživatele

Musí existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.

Registrace uživatele se vede v centrální databázi uživatelů (osobní čísla). Aktualizace se provádí podle systému SAP každý den automaticky.

A.11.2.2 Řízení privilegovaného přístupu

Přidělování a používání privilegií musí být omezeno a řízeno.

Privilegovaný přístup je omezen výhradně na administrátory.

A.11.2.3 Správa uživatelských hesel

Přidělování hesel musí být řízeno formálním procesem.

Uživatelská hesla jsou přidělována správně, struktura hesla je dána pravidly, která jsou prosazována informačním systémem, je vyžadována pravidelná změna hesla. Řešení je na dobré úrovni.

A.11.2.4 Přezkoumání přístupových práv uživatelů

Vedení organizace musí v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.

Přístupová práva se nepřezkoumávají, pouze se kontrolují platnosti účtů podle systému SAP. Takové řízení je nedostatečné, měly by se pravidelně přezkoumávat potřeby přístupu k aktivům. Měl by být zaveden princip „vlastnictví aktiv“.

A.11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací.

A.11.3.1 Používání hesel

Při výběru a používání hesel musí být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy.

Struktura hesla je dána pravidly, která jsou prosazována informačním systémem, je vyžadována pravidelná změna hesla.

A.11.3.2 Neobsluhovaná uživatelská zařízení

Uživatelé musí zajistit přiměřenou ochranu neobsluhovaných zařízení.

Pro neobsluhovaná zařízení nejsou stanovena pravidla s výjimkou spořiče obrazovky, který se zapíná po 30 minutách nečinnosti. Ochrana nepoužívaných portů apod. není řešena.

A.11.3.3 Zásada prázdného stolu a prázdné obrazovky monitoru

Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.

Pro tuto problematiku nejsou stanovena pravidla s výjimkou spořiče obrazovky. Pravidlo čistého stolu není u společnosti zavedeno. Toto pravidlo znamená téměř nulové náklady a významné posílení bezpečnosti.

A.11.4 Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám.

A.11.4.1 Politika užívání síťových služeb

Uživatelé musí mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.

Přístup k síťovým zdrojům povoluje nadřízený zaměstnance. Na technické úrovni se řízení přístupu realizuje zejména na aplikační vrstvě.

A.11.4.2 Autentizace uživatele pro externí připojení

Přístup vzdálených uživatelů musí být odpovídajícím způsobem autentizován.

Přístup k síťovým zdrojům je řešen prostřednictvím VPN, která prostřednictvím kryptografického zabezpečení zajišťuje autenticitu připojovaného uživatele.

A.11.4.3 Identifikace zařízení v sítích

Pro autentizaci připojení z vybraných lokalit a zařízení musí být zváženo použití automatické identifikace zařízení.

IP adresa zařízení je svázána s MAC adresou. Tato vazba je využívána DHCP serverem, což poskytuje jistou míru autentizace zařízení v síti.

A.11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Fyzický i logický přístup k diagnostickým a konfiguračním portům musí být řízen.

Fyzický přístup k portům je zabezpečen omezením přístupu osob do prostor IT. Logický přístup k diagnostickým a konfiguračním portům je zabezpečen firewallem, který je spravován externí firmou, takže bezpečnost je do značné míry závislá na způsobu nastavení závazků a odpovědnosti této firmy vůči společnosti.

A.11.4.5 Princip oddělení v sítích

Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích odděleny.

Síť je rozdělena do 5 subsítí. Ochrana na této úrovni není řešena.

A.11.4.6 Řízení síťových spojení

U sdílených sítí, zejména těch, které přesahují hranice organizace, musí být omezeny možnosti připojení uživatelů. Omezení musí být v souladu s politikou řízení přístupu a s požadavky aplikací.

Uvnitř sítě nejsou instalovány brány pro filtrování provozu. Tato brána existuje jen mezi vnitřní a externí sítí (firewall).

A.11.4.7 Řízení směrování sítě

Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, musí být zavedeno řízení směrování sítě.

V síti je jeden centrální přepínač L3 (analyzuje protokol IP 3. vrstvy OSI modelu a funguje jako směrovač), ostatní přepínače jsou úrovně L2. Přepínače na úrovni L4 (umí analyzovat protokol 4. vrstvy OSI modelu a zpracovávat pakety např. podle čísel portů) u společnosti instalován není. Směrování sítě s ohledem na informační toky ve společnosti zavedeno není.

A.11.5 Řízení přístupu k operačnímu systému

Cíl: Předcházet neautorizovanému přístupu k operačním systémům.

A.11.5.1 Bezpečné postupy přihlášení

Přístup k operačnímu systému musí být řízen postupy bezpečného přihlášení.

Postupy bezpečného přihlášení jsou ve společnosti implementovány.

A.11.5.2 Identifikace a autentizace uživatelů

Všichni uživatelé musí mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), musí být také zvolen vhodný způsob autentizace k ověření jejich identity.

Požadavek je ve společnosti implementován.

A.11.5.3 Systém správy hesel

Systém správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.

Požadavek je ve společnosti implementován.

A.11.5.4 Použití systémových nástrojů

Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly, musí být omezeno a přísně kontrolováno.

Požadavek je ve společnosti implementován, takové nástroje mohou použít jen administrátoři.

A.11.5.5 Časové omezení relace

Neaktivní relace se musí po stanovené době nečinnosti ukončit.

Pro uživatele je nataven standardní čas připojení od 05:00 do 23:00. Výjimky musí být explicitně povolovány.

A.11.5.6 Časové omezení spojení

U vysoce rizikových aplikací musí být pro zajištění dodatečné bezpečnosti použito omezení doby spojení.

Spojení není časově omezováno. Není důvod aplikovat toto opatření.

A.11.6 Řízení přístupu k aplikacím a informacím

Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.

A.11.6.1 Omezení přístupu k informacím

Uživatelé aplikačních systémů, včetně pracovníků podpory, musí mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu.

Je zavedeno řízení přístupu uživatelů a schvalovací mechanismy pro povolování přístupu uživatelů k informacím.

A.11.6.2 Oddělení citlivých systémů

Citlivé aplikační systémy musí mít oddělené (izolované) počítačové prostředí.

U společnosti není žádný systém deklarován jako „citlivý“. Opatření není aplikováno.

A.11.7 Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku.

A.11.7.1 Mobilní výpočetní zařízení a sdělovací technika

Musí být ustavena formální pravidla a přijata bezpečnostní opatření na ochranu proti rizikům používání mobilních výpočetních a komunikačních zařízení.

Pravidla pro používání mobilní techniky u společnosti nejsou formulována.

A.11.7.2 Práce na dálku

Organizace musí vytvořit a do praxe zavést zásady, operativní plány a postupy pro práci na dálku.

Práce na dálku se teprve začíná rozvíjet. Technicky je bezpečnost zajištěna prostřednictvím VPN, která poskytuje dostatečné záruky za autenticitu připojení zvenčí. Jsou nedostatečně formulována pravidla.

A.12 Akvizice, vývoj a údržba informačních systému

A.12.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost stala nedílnou součástí informačních systémů.

A.12.1.1 Analýza a specifikace bezpečnostních požadavků

Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů musí obsahovat také požadavky na bezpečnostní opatření.

U společnosti se takovéto analýzy neprovádějí. Byla provedena jediná bezpečnostní analýza informačního systému, bezpečnostní analýzy se neprovádějí periodicky. Bezpečnost u společnosti není řešena prostřednictvím řízení rizik. Opatření není implementováno.

A.12.2 Správné zpracování v aplikacích

Cíl: Předcházet chybám, ztrátě, neoprávněné modifikaci nebo zneužití informací v aplikacích.

A.12.2.1 Validace vstupních dat

Vstupní data aplikací musí být kontrolována z hlediska správnosti a adekvátnosti.

Kontrola vstupních dat je prováděna aplikacemi. Opatření je implementováno.

A.12.2.2 Kontrola vnitřního zpracování

Pro detekci jakéhokoliv poškození informací vzniklého chybami při zpracování nebo úmyslnými zásahy musí být začleněny kontroly validace dat do aplikace.

Opatření není implementováno.

A.12.2.3 Integrita zpráv

U jednotlivých aplikací musí být stanoveny požadavky na zajištění autentizace a integrity zpráv a podle potřeby identifikována a zavedena vhodná opatření.

Opatření není implementováno.

A.12.2.4 Kontrola výstupních dat

Pro zajištění toho, že zpracování uložených informací je bezchybné a odpovídající dané situaci, musí být provedeno ověření platnosti výstupních dat z aplikace.

Opatření je implementováno jedině u problematiky mezd a je prováděno jedině mzdovou účtárnou. Není doloženo, zda by toto opatření nemělo být implementováno i jinde.

A.12.3 Kryptografická opatření

Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.

U společnosti se kryptografické prostředky systematicky nepoužívají. Používají se pouze individuálně (např. PGP).

A.12.3.1 Politika pro použití kryptografických opatření

Musí být vytvořena a zavedena politika pro používání kryptografických opatření na ochranu informací.

Opatření není implementováno.

A.12.3.2 Správa klíčů

Na podporu používání kryptografických technik v organizaci musí existovat systém správy klíčů.

Opatření není implementováno.

A.12.4 Bezpečnost systémových souborů

Cíl: Zajistit bezpečnost systémových souborů.

A.12.4.1 Správa provozního programového vybavení

Musí být zavedeny postupy pro kontrolu instalace programového vybavení na provozních systémech.

Používá se automatická kontrola instalace programového vybavení produktem ZENworks. Opatření je aplikováno.

A.12.4.2 Ochrana systémových testovacích údajů

Testovací data musí být pečlivě vybrána, chráněna a kontrolována.

Při testování se používají ostrá data, která nejsou anonymizována. Ochrana těchto dat je stejná jako v provozním systému. Nejsou stanoveny procedury pro bezpečnou likvidaci testovacích dat. Požadavek je implementován částečně.

A.12.4.3 Řízení přístupu ke knihovně zdrojových kódů

Přístup ke knihovně zdrojových kódů musí být omezen.

Přístup je omezen jen na administrátory, kteří mají jediní znalostní potenciál ke zneužití zdrojových kódů. V rámci administrátorů není zaveden princip „need to know“[1]. Požadavek je implementován částečně.

A.12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost programového vybavení a informací aplikačních systémů.

A.12.5.1 Postupy řízení změn

Musí být zavedeny formální postupy řízení změn.

Řízení změn je realizováno prostřednictvím aplikace Intranet. Opatření je z velké části zavedeno.

A.12.5.2 Technické přezkoumání aplikací po změnách operačního systému

V případě změny operačního systému musí být přezkoumány a otestovány kritické aplikace, aby bylo zajištěno, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.

Opatření není zcela implementováno, nejsou stanovena pravidla, řeší se případ od případu.

---

[1] „need to know“ – přístup k informacím není povolen, dokud není nezbytný pro splnění konkrétního oficiálního úkolu

A.12.5.3 Omezení změn programových balíků

Modifikace programových balíků musí být omezeny pouze na nezbytné změny, veškeré prováděné změny musí být řízeny.

Opatření je z velké části zavedeno. Používá se automatická kontrola instalace programového vybavení produktem ZENworks.

A.12.5.4 Unik informací

Musí být zabráněno příležitostem k úniku informací.

Problematika reakce na únik informací není řešena, chybí metodika reakce na tuto situaci.

A.12.5.5 Programové vybavení vyvíjené externím dodavatelem

Organizace musí dohlížet a monitorovat vývoj programového vybavení externím dodavatelem.

Opatření není implementováno.

A.12.6 Řízení technických zranitelností

Cíl: Snížit rizika vyplývající z využívání zveřejněných technických zranitelností.

A.12.6.1 Řízení, správa a kontrola technických zranitelností

Musí být zajištěno včasné získání informací o existenci technických zranitelností v provozovaném informačním systému, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na pokrytí souvisejících rizik.

Opatření je řešeno jen částečně. Administrátoři sledují odborný tisk a zúčastňují se některých kurzů a konferencí. Takto získané informace jsou aplikovány do IS a podnikají se nápravná opaření vůči nově zjištěným rizikům. Tento proces ale není systematicky řízen a plánován.

A.13 Zvládání bezpečnostních incidentů

A.13.1 Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

Tato problematika není u společnosti formálně řešena.

A.13.1.1 Hlášení bezpečnostních událostí

Bezpečnostní události musí být co nejrychleji hlášeny příslušnými řídícími kanály.

Opatření není implementováno.

A.13.1.2 Hlášení bezpečnostních slabin

Všichni zaměstnanci, smluvní strany a ostatní uživatelé informačního systému a služeb musí být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.

Opatření není implementováno.

A.13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

Tato problematika není u společnosti formálně řešena. Bezpečnostní incidenty a kroky k nápravě se řeší nahodile případ od případu.

A.13.2.1 Odpovědnosti a postupy

Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty musí být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.

Opatření není implementováno.

A.13.2.2 Ponaučení z bezpečnostních incidentů

Musí existovat mechanizmy, které by umožňovaly kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů.

Opatření není implementováno.

A.13.2.3 Shromaždování důkazů

V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (podle práva občanského nebo trestního) vůči osobě anebo organizaci, musí být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat.

Opatření není implementováno.

A.14 Řízení kontinuity činností organizace

A.14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Cíl: Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činností.

Plány řízení kontinuity IS nejsou u společnosti zpracovány.

A.14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace

V rámci organizace musí existovat řízený proces pro rozvoj a udržování kontinuity činností organizace.

Opatření není implementováno.

A.14.1.2 Kontinuita činností organizace a hodnocení rizik

Musí být identifikovány možné příčiny přerušení činností organizace, včetně jejich pravděpodobnosti, velikosti dopadu a možných následků na bezpečnost informací.

Opatření není implementováno.

A.14.1.3 Vytváření a implementace plánů kontinuity

Pro udržení nebo obnovení provozních činností organizace po přerušení nebo selhání kritických procesů a pro zajištění dostupnosti informací v požadovaném čase a na požadovanou úroveň musí být vytvořeny a implementovány plány.

Opatření není implementováno.

A.14.1.4 Systém plánování kontinuity činností organizace

Pro zajištění konzistence plánů kontinuity činností a pro určení priorit testování a údržby musí být k dispozici jednotný systém plánů kontinuity činností organizace.

Opatření není implementováno.

A.14.1.5 Testování, udržování a přezkoumání plánů kontinuity

Plány kontinuity činností organizace musí být pravidelně testovány a aktualizovány, aby se zajistila jejich aktuálnost a efektivnost.

Opatření není implementováno.

A.15 Soulad s požadavky

A.15.1 Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

A.15.1.1 Identifikace odpovídajících předpisů

Pro každý informační systém musí být jednoznačně definovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, regulatorní a smluvní požadavky a způsob, jakým je organizace dodržuje.

Požadavek je řešen v rámci implementace standardu ISO 9001.

A.15.1.2 Ochrana duševního vlastnictví

Pro zajištění souladu se zákonnými, regulatorními a smluvními požadavky na použití materiálů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví, musí být zavedeny vhodné postupy.

Opatření není implementováno.

A.15.1.3 Ochrana záznamů organizace

Důležité záznamy organizace musí být chráněny proti ztrátě, zničení a padělání a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.

Opatření není implementováno.

A.15.1.4 Ochrana dat a osobních údajů

Ochrana dat a soukromí musí být zajištěna v souladu s odpovídající legislativou, předpisy, a pokud je to relevantní, se smlouvami.

Opatření je řešeno ve směrnici OS-6-12 „Ochrana osobních údajů“. Opatření je implementováno.

A.15.1.5 Prevence zneužití prostředků pro zpracování informací

Musí být zakázáno používat prostředky pro zpracování informací jiným než autorizovaným způsobem.

Přístup k aktivům je autorizován vedoucími zaměstnanci prostřednictvím aplikace Intranet. Rezervy jsou ve školení zaměstnanců a v monitorování užití prostředků IS.

A.15.1.6 Regulace kryptografických opatření

Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, zákony a předpisy.

Opatření není implementováno.

A.15.2 Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.

A.15.2.1 Shoda s bezpečnostními politikami a normami

Vedoucí zaměstnanci musí zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami.

Shoda s normami se kontroluje pouze v rámci realizace ISO 9001. Audit se provádí u systému SAP při finanční kontrole. Audit bezpečnosti údajně proběhl před 5 lety.

A.15.2.2 Kontrola technické shody

Informační systémy musí být pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy.

Opatření není implementováno.

A.15.3 Hlediska auditu informačních systémů

Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do/z informačních systémů.

A.15.3.1 Opatření k auditu informačních systémů

Požadavky auditu a činnosti zahrnující kontrolu provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace.

Opatření není implementováno.

A.15.3.2 Ochrana nástrojů pro audit informačních systémů

Přístup k nástrojům určeným pro audit informačních systémů musí být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.

Opatření není implementováno.

3.2 Výpočet míry plnění

Hodnoty získané během auditu jsem dosadila do vzorce (2.3), čímž jsem vypočetla míry plnění pro jednotlivé cíle ISMS (viz. Tab. 3.1).

A.5.1	Bezpečnostní politika informací	20
A.6.1	Interní organizace	63
A.6.2	Externí subjekty	33
A.7.1	Odpovědnost za aktiva	33
A.7.2	Klasifikace informací	0
A.8.1	Před vznikem pracovního vztahu	47
A.8.2	Během pracovního vztahu	67
A.8.3	Ukončení nebo změna pracovního vztahu	73
A.9.1	Zabezpečené oblasti	87
A.9.2	Bezpečnost zařízení	60
A.10.1	Provozní postupy a odpovědnosti	50
A.10.2	Řízení dodávek služeb třetích stran	27
A.10.3	Plánování a přejímání systémů	70
A.10.4	Ochrana proti škodlivým programům a mobilním kódům	90
A.10.5	Zálohování	100
A.10.6	Správa bezpečnosti sítě	100
A.10.7	Bezpečnost při zacházení s médii	15
A.10.8	Výměna informací	32
A.10.9	Služby elektronického obchodu	0
A.10.10	Monitorování	50
A.11.1	Požadavky na řízení přístupu	80
A.11.2	Řízení přístupu uživatelů	85
A.11.3	Odpovědnosti uživatelů	40
A.11.4	Řízení přístupu k síti	69
A.11.5	Řízení přístupu k operačnímu systému	83
A.11.6	Řízení přístupu k aplikacím a informacím	50
A.11.7	Mobilní výpočetní zařízení a práce na dálku	40
A.12.1	Bezpečnostní požadavky informačních systémů	0
A.12.2	Správné zpracování v aplikacích	35
A.12.3	Kryptografická opatření	0
A.12.4	Bezpečnost systémových souborů	73
A.12.5	Bezpečnost procesů vývoje a podpory	36
A.12.6	Řízení technických zranitelností	60
A.13.1	Hlášení bezpečnostních událostí a slabin	0
A.13.2	Zvládání bezpečnostních incidentů a kroky k nápravě	0
A.14.1	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	0
A.15.1	Soulad s právními normami	43
A.15.2	Soulad s bezpečnostními politikami, normami a technická shoda	30
A.15.3	Hlediska auditu informačních systémů	0

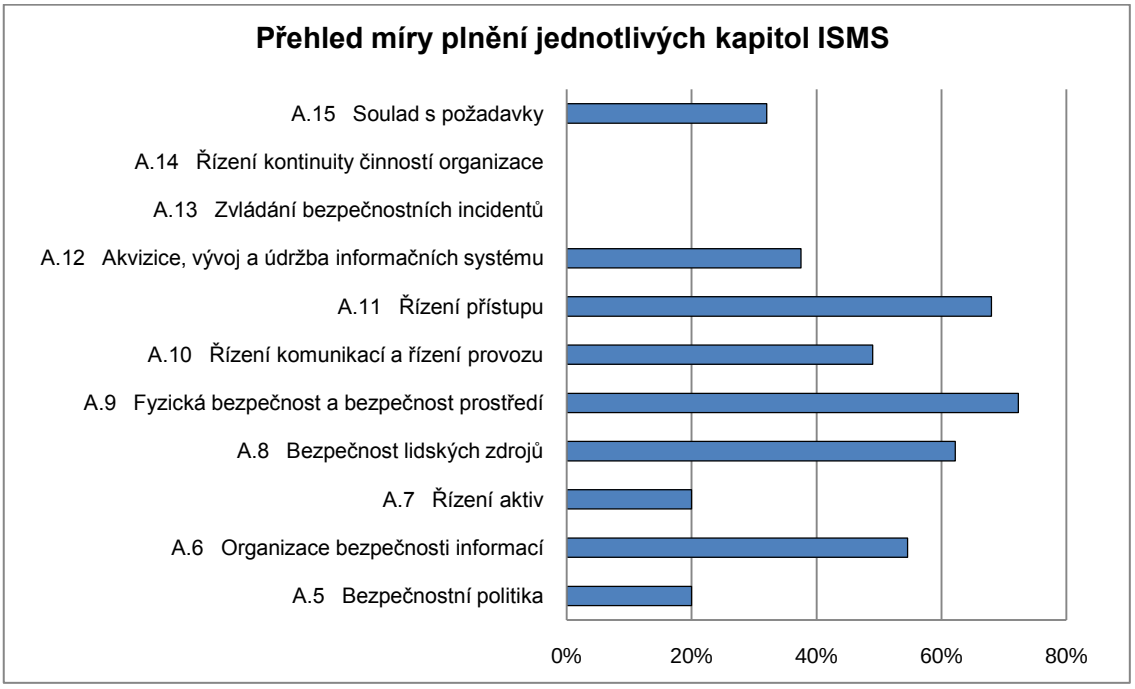
Tab. 3.1 Míry plnění jednotlivých cílů ISMS

Z těchto hodnot jsem pak pomocí vzorce (2.4) vypočetla míru plnění ISMS. Výsledné hodnocení řízení bezpečnosti pro společnost Výrobní podnik a.s. je tedy 44,6 %.

$$MP_{ISMS} = \frac{\text{Součet měr plnění všech cílů ISMS}}{\text{Počet cílů v ISMS}} = \frac{1740,7}{39} = \mathbf{44,6\ \%}$$

3.3 Shrnutí

Ve společnosti Výrobní podnik a.s. byly zjištěny závažné nedostatky vůči normě ISO/IEC 27001:2005, což se projevilo i nízkou hodnotou shody s požadavky tohoto standardu. Bezpečnost je v jednotlivých oblastech často řešena spíše nahodile a v důsledku toho u společnosti nejsou trvale monitorována, řízena a periodicky vyhodnocována rizika a chybí také zpětné ověřování účinnosti bezpečnostních opatření. Kapitoly řízení kontinuity činností organizace a zvládání bezpečnostních incidentů nejsou zavedeny vůbec (viz. Obr. 3.2).



Obr. 3.2 Přehled míry plnění jednotlivých kapitol ISMS

Společnost by měla zavést systém řízení informační bezpečnosti, který by definoval postupy pro plánování, zavedení, kontrolu a zlepšování jednotlivých procesů tohoto systému. Díky těmto postupům by bylo možné průběžné hodnotit účinnost zavedených bezpečnostních opatření a společnost by získala nástroj na odpovědné řízení rizik v rámci systému.

Předpokladem pro úspěšnou implementaci ISMS je zavedení systému řízení rizik. Společnost by tedy v první řadě měla provést identifikaci, analýzu a vyhodnocení rizik, kterým jsou vystavena důležitá informační aktiva, a zavést opatření pro minimalizaci následků v případě bezpečnostních incidentů.

Návrh konkrétních opatření na ochranu informačních aktiv společnosti přesahuje rozsah této práce.

Závěr

Řízení bezpečnosti informací je základem úspěšného chodu každé větší firmy i státní instituce. V dnešní době představují informace jedno z nejcennějších aktiv společnosti a jejich ochrana neznamená pouze konkurenční výhodu, ale stává se i nutností pro další působení firmy na trhu. Finanční ztráty plynoucí z bezpečnostních incidentů jsou jen jedním z mnoha následků, které firmám v případě nedostatečné ochrany informačních aktiv hrozí.

Cílem této práce bylo prověřit systém řízení bezpečnosti informací ve společnosti Výrobní podnik a.s. a upozornit na možné zranitelnosti, které se v tomto systému objevují. Z výsledků auditu je patrné, že zavádění systému řízení neprobíhalo podle normy ISO/IEC 27001:2005, ale spíše nahodile v důsledku bezpečnostních incidentů nebo zjištění pracovníků, kteří jsou za bezpečnost ve firmě odpovědní. Tento způsob má mnoho nedostatků a neumožňuje zpětnou kontrolu účinnosti již zavedených bezpečnostních opatření. V řízení bezpečnosti byly navíc identifikovány oblasti, které nesplňovaly žádná bezpečnostní opatření.

Jako řešení chybějících bezpečnostních opatření jsem doporučila firmě zavést systém řízení rizik, který se věnuje identifikaci důležitých informačních aktiv, analýze rizik, kterým jsou tato aktiva vystavena, a implementaci opatření pro minimalizaci následků případných bezpečnostních incidentů. Na základě výsledků auditu se společnost rozhodla podstoupit kroky pro zavedení systému řízení rizik a byl vytvořen návrh projektu, který bude zařazen do programu rozvoje společnosti v příštím roce.

Seznam použité literatury

a) tištěné publikace:

[1] ANDERSON, R., J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Wiley Publishing, 2008. 1080 s. ISBN 978-0-470-06852-6.

[2] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky: Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2006. 36 s.

[3] ČSN ISO/IEC 17799. *Informační technologie – Bezpečnostní techniky: Soubor postupů pro management bezpečnosti informací*. Praha: Český normalizační institut, 2006. 102 s.

[4] ČSN EN ISO 19011. *Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu*. Praha: Český normalizační institut, 2003. 56 s.

[5] ŠEBESTA, V.; ŠTVERKA, V.; STEINER, F.; ŠEBESTOVÁ, M. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. 1. vyd. Praha: Český normalizační institut, 2006. 70 s. ISBN 80-7283-204-2.

[6] KOPÁČIK, I. a kol. *Riadenie a audit v informačnej bezpečnosti.* 1. vyd. Bratislava: TATE International Slovakia, s.r.o., 2007. 322 s. ISBN 978-80-969747-0-2.

[7] POKORNÝ, P. *Základy psychologie a komunikace pro auditory IS.* 1. vyd. Praha: Certification & Information Security Services, 2006. 19 s.

b) elektronické zdroje:

[8] CHLUP, Marek. Hrozby? A co s nimi? *Gity: Bezpečnost v kostce* [online]. 2005 [cit. 2010-01-06]. Dostupný z WWW: < http://www.chrantesidata.cz/cs/art/1153-dil-6/>.

Seznam zkratek a symbolů

IS – informační systém

HW – technické vybavení počítače

ISMS – systém managementu bezpečnosti informací

IS/ICT – informační systémy a informační a komunikační technologie

IT – informační technologie

ISO – mezinárodní organizace pro normalizaci

IEC – mezinárodní elektrotechnická komise

THP – technicko-hospodářský pracovník

SAP – soubor podnikových aplikací a obchodních řešení pro podporu podnikání

MAC – kontrola přístupu k médiu

IP – internetový protokol

DHCP – protokol dynamické konfigurace hostitele

SQL – strukturovaný dotazovací jazyk

VPN – virtuální privátní síť

MP – míra plnění

H – hodnocení

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……

……
jméno a příjmení studenta

Adresa trvalého pobytu studenta:

U Lesa 701
Vřesina
742 85

Seznam příloh

Příloha č. 1: Bezpečnostní politika informací (dokument)

Bezpečnostní politika informací[1]

(VZOR)

Cíle

Cílem bezpečnostní politiky informací je zajistit kontinuitu podnikání a minimalizovat obchodní ztráty důslednou prevencí a minimalizací dopadů informačních incidentů.

Politika

- Záměrem této Politiky je **chránit informační aktiva organizace před všemi hrozbami**, ať už interními nebo externími, záměrnými nebo náhodnými.
- Tato politika byla schválena výkonným ředitelem společnosti.
- Politika bezpečnosti informací je zárukou, že
  - Informace budou **chráněny proti neautorizovanému přístupu**;
  - **Důvěrnost** informací je zajištěna;
  - **Integrita** informací je udržována;
  - **Dostupnost** informací je zajištěna tak, jak požadují obchodní postupy organizace;
  - **Zákonné a legislativní předpisy** jsou dodržovány;
  - **Plán obnovy obchodních činností** organizace je vypracován, udržován a testován;
  - **Školení a výcvik v oblasti informační bezpečnosti** budou dostupné všem pracovníkům organizace;
  - **Všechna narušení bezpečnosti informací**, skutečná nebo potenciální, budou oznamována a přešetřována **bezpečnostním manažerem organizace**;
- Existují pracovní postupy pro podporu této politiky. Ty zahrnují bezpečnostní postupy proti zlovolnému software, pro používání hesel a kontinuitu obchodu.
- Požadavky na obchodní činnost organizace z hlediska dostupnosti informací a informačních systémů jsou respektovány.
- Manažer informační bezpečnosti je přímo odpovědný za dodržování této politiky a poskytování instrukcí a návodů pro její implementaci.
- Všichni vedoucí pracovníci jsou přímo odpovědni za implementaci politiky bezpečnosti informací v oblasti jejich obchodních aktivit a za její dodržování jemu podřízenými osobami.
- Povinností všech zaměstnanců je dodržovat postupy, stanovené touto politikou.

Tato politika bude přezkoumávána bezpečnostním ředitelem společnosti minimálně jednou ročně.

Schvalovací doložka

	Jméno	datum	podpis
Vypracoval:			
Přezkoumal:			
Schválil:			

[1] *Oblast standardu ČSN ISO/IEC 27001:2006.* 1. vyd. Praha: Certification & Information Security Services, 2006. 98 s.

Příloha č. 2: Přehled hodnocení jednotlivých opatření (tabulka)

Požadavky normy ISO/IEC 27001:2005			*H*
A.5	**Bezpečnostní politika**		
A.5.1	**Bezpečnostní politika informací**	*Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a směrnicemi.*	
A.5.1.1	Dokument bezpečnostní politiky informací	*Dokument bezpečnostní politiky informací musí být schválen vedením organizace, publikován a dán na vědomí všem zaměstnancům a relevantním externím stranám.*	40
A.5.1.2	Přezkoumání bezpečnostní politiky informací	*Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti musí být bezpečnostní politika informací přezkoumávána v plánovaných intervalech a vždy když nastane významná změna.*	0
	Míra plnění daného cíle		20
A.6	**Organizace bezpečnosti informací**		
A.6.1	**Interní organizace**	*Cíl: Řídit bezpečnost informací v organizaci.*	
A.6.1.1	Závazek vedení směrem k bezpečnosti informací	*Vedení organizace musí stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace. Mělo by demonstrovat svůj závazek a jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací.*	20
A.6.1.2	Koordinace bezpečnosti informací	*Činnosti v oblasti bezpečnosti informací musí být koordinovány prostřednictvím zástupců různých útvarů z celé organizace s odpovídajícími rolemi a pracovním zařazením.*	40
A.6.1.3	Přidělení odpovědností v oblasti bezpečnosti informací	*Musí být jasně definovány odpovědnosti v oblasti bezpečnosti informací.*	100
A.6.1.4	Schvalovací proces prostředků pro zpracování informací	*Musí být stanoven a zaveden postup schvalování (vedoucími zaměstnanci) nových prostředků pro zpracování informací.*	60
A.6.1.5	Dohody o ochraně důvěrných informací	*Musí být určeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.*	80
A.6.1.6	Kontakt s orgány veřejné správy	*Musí být udržovány přiměřené vztahy s orgány veřejné správy.*	100
A.6.1.7	Kontakt se zájmovými skupinami	*Musí být udržovány přiměřené vztahy se zájmovými skupinami nebo speciálními fóry na bezpečnost a profesními sdruženími.*	100
A.6.1.8	Nezávislá přezkoumání bezpečnosti informací	*Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cíle opatření, jednotlivá opatření, politiky, směrnice a postupy) musí být v pravidelných intervalech (anebo v případě jakékoliv významné změny ve vztahu k bezpečnosti) nezávisle přezkoumávány.*	0
	Míra plnění daného cíle		63
A.6.2	**Externí subjekty**	*Cíl: Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.*	
A.6.2.1	Identifikace rizik plynoucích z přístupu externích subjektů	*Předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací, musí být identifikována rizika a implementována vhodná opatření na jejich pokrytí.*	20

A.6.2.2	Bezpečnostní požadavky pro přístup klientů	*Předtím, než je klientům umožněn přístup k informacím nebo aktivům organizace, musí být identifikované všechny požadavky na bezpečnost*	40
A.6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	*Dohody, uzavřené s třetími stranami zahrnující přístup, zpracování, sdělování nebo správu informací organizace nebo správu prostředků pro zpracování informací, případně dodávku produktů nebo služeb k zařízení pro zpracování informací, musí pokrývat veškeré relevantní bezpečnostní požadavky.*	40
	Míra plnění daného cíle		33
A.7	**Řízení aktiv**		
A.7.1	**Odpovědnost za aktiva**	*Cíl: Nastavit a udržovat přiměřenou ochranu aktiv organizace.*	
A.7.1.1	Evidence aktiv	*Musí být jasně identifikována všechna aktiva organizace, všechna důležitá aktiva musí být evidována a seznam udržován aktuální.*	0
A.7.1.2	Vlastnictví aktiv	*Veškeré informace a aktiva související s prostředky pro zpracování informací musí mít určeného vlastníka.*	0
A.7.1.3	Přípustné použití aktiv	*Musí být určena, dokumentována a do praxe zavedena pravidla pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.*	100
	Míra plnění daného cíle		33
A.7.2	**Klasifikace informací**	*Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany.*	
A.7.2.1	Doporučení pro klasifikaci	*Informace musí být klasifikovány a to ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.*	0
A.7.2.2	Označování a nakládání s informacemi	*Pro označování informací a zacházení s nimi musí být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.*	0
	Míra plnění daného cíle		0
A.8	**Bezpečnost lidských zdrojů**		
A.8.1	**Před vznikem pracovního vztahu**	*Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.*	
A.8.1.1	Role a odpovědnosti	*Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací musí být definovány a dokumentovány v souladu s bezpečnostní politikou organizace.*	60
A.8.1.2	Prověřování	*Všichni uchazeči o zaměstnání, smluvní a třetí strany musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti a potenciálních rizik.*	0
A.8.1.3	Podmínky výkonu pracovní činnosti	*Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami musí obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.*	80
	Míra plnění daného cíle		47

A.8.2	**Během pracovního vztahu**	*Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.*	
A.8.2.1	Odpovědnosti vedoucích zaměstnanců	*Vedoucí zaměstnanci musí po uživatelích, smluvních a třetích stranách požadovat dodržování bezpečnosti v souladu se zavedenými politikami a postupy.*	80
A.8.2.2	Informovanost, vzdělávání a školení v oblasti bezpečnosti informací	*Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran musí, s ohledem na svou pracovní náplň, absolvovat odpovídající a pravidelně se opakující školení v oblasti bezpečnosti informací, bezpečnostní politiky a směrnic organizace.*	80
A.8.2.3	Disciplinární řízení	*Musí existovat formalizované disciplinární řízení vůči zaměstnancům, kteří se dopustili narušení bezpečnosti.*	40
	Míra plnění daného cíle		67
A.8.3	Ukončení nebo změna pracovního vztahu	*Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.*	
A.8.3.1	Odpovědnosti při ukončení pracovního vztahu	*Musí být jasně určeny a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu.*	80
A.8.3.2	Navrácení zapůjčených předmětů	*Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené předměty, které jsou majetkem organizace.*	100
A.8.3.3	Odebrání přístupových práv	*Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna přístupová práva k informacím a prostředkům pro zpracování informací.*	40
	Míra plnění daného cíle		73
A.9	**Fyzická bezpečnost a bezpečnost prostředí**		
A.9.1	**Zabezpečené oblasti**	*Cíl: Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.*	
A.9.1.1	Fyzický bezpečnostní perimetr	*Při ochraně prostor, ve kterých se nachází informace nebo prostředky pro zpracování informací, musí být používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).*	100
A.9.1.2	Fyzické kontroly vstupu osob	*Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.*	100
A.9.1.3	Zabezpečení kanceláří, místností a prostředků	*Musí být navrženo a aplikováno fyzické zabezpečení kanceláří, místností a prostředků.*	100
A.9.1.4	Ochrana před hrozbami vnějšku a prostředí	*Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami, musí být navrženy a aplikovány prvky fyzické ochrany.*	100
A.9.1.5	Práce v zabezpečených oblastech	*Pro práci v zabezpečených oblastech musí být navrženy a aplikovány prvky fyzické ochrany.*	100

A.9.1.6	Veřejný přístup, prostory pro nakládku a vykládku	*Prostory pro nakládku a vykládku a další místa, kudy se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolována a pokud možno by měla být izolována od prostředků pro zpracování informací tak, aby se zabránilo neoprávněnému přístupu k nim*	20
	Míra plnění daného cíle		87
A.9.2	**Bezpečnost zařízení**	*Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.*	
A.9.2.1	Umístění zařízení a jeho ochrana	*Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.*	100
A.9.2.2	Podpůrná zařízení	*Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.*	20
A.9.2.3	Bezpečnost kabelových rozvodů	*Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem či poškozením.*	100
A.9.2.4	Údržba zařízení	*Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.*	100
A.9.2.5	Bezpečnost zařízení mimo prostory organizace	*Zařízení používané mimo prostory organizace musí být zabezpečeno s přihlédnutím k různým rizikům, která vyplývají z jeho použití mimo organizaci.*	20
A.9.2.6	Bezpečná likvidace nebo opakované použití zařízení	*Všechna zařízení obsahující paměťová média musí být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna nebo bezpečně přepsána.*	20
A.9.2.7	Přemístění majetku	*Zařízení, informace nebo programové vybavení nesmí být bez předchozího schválení přemisťováno.*	60
	Míra plnění daného cíle		60
A.10	**Řízení komunikací a řízení provozu**		
A.10.1	**Provozní postupy a odpovědnosti**	*Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.*	
A.10.1.1	Dokumentace provozních postupů	*Provozní postupy musí být zdokumentovány a udržovány a musí být dostupné všem uživatelům podle potřeby.*	20
A.10.1.2	Řízení změn	*Změny systémů a prostředků pro zpracování informací musí být řízeny.*	60
A.10.1.3	Oddělení povinností	*Pro snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení jednotlivých povinností a odpovědností.*	60
A.10.1.4	Oddělení vývoje, testování a provozu	*Pro snížení rizika neoprávněného přístupu k provoznímu systému anebo jeho změn musí být zajištěno oddělení prostředků vývoje, testování a provozu.*	60
	Míra plnění daného cíle		50
A.10.2	**Řízení dodávek služeb třetích stran**	*Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávání služeb ve shodě s uzavřenými dohodami.*	
A.10.2.1	Dodávky služeb	*Musí být zajištěno, aby bezpečnostní opatření, definice a úroveň poskytovaných služeb, byly třetí stranou implementovány, provozovány a udržovány ve shodě s uzavřenými dohodami.*	40

A.10.2.2	Monitorování a přezkoumávání služeb třetích stran	*Služby, zprávy a záznamy poskytované třetí stranou musí být pravidelně monitorovány a přezkoumávány, audity musí být opakovány v pravidelných intervalech.*	20
A.10.2.3	Řízení změn služeb poskytovaných třetími stranami	*Změny v poskytování služeb, včetně udržování a zlepšování existujících bezpečnostních politik, postupů a bezpečnostních opatření, musí být řízeny s ohledem na kritičnost systémů a procesů organizace, které jsou součástí opakovaného hodnocení rizik.*	20
	Míra plnění daného cíle		27
A.10.3	**Plánování a přejímání systémů**	*Cíl: Minimalizovat riziko selhání systémů.*	
A.10.3.1	Řízení kapacit	*Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.*	60
A.10.3.2	Přejímání systémů	*Musí být určena kritéria pro přejímání nových informačních systémů, jejich aktualizaci a zavádění nových verzí a vhodný způsob testování systému v průběhu vývoje a před zavedením do ostrého provozu.*	80
	Míra plnění daného cíle		70
A.10.4	**Ochrana proti škodlivým programům a mobilním kódům**	*Cíl: Chránit integritu programového vybavení a dat.*	
A.10.4.1	Opatření na ochranu proti škodlivým programům	*Na ochranu proti škodlivým programům a nepovoleným mobilním kódům musí být implementována na jejich detekci, prevenci a obnovu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.*	100
A.10.4.2	Opatření na ochranu proti mobilním kódům	*Použití povolených mobilních kódů musí být nastaveno v souladu s bezpečnostní politikou, musí být zabráněno spuštění nepovolených mobilních kódů.*	80
	Míra plnění daného cíle		90
A.10.5	**Zálohování**	*Cíl: Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.*	
A.10.5.1	Zálohování informací	*Záložní kopie důležitých informací a programového vybavení organizace musí být pořizovány a testovány v pravidelných intervalech.*	100
	Míra plnění daného cíle		100
A.10.6	**Správa bezpečnosti sítě**	*Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.*	
A.10.6.1	Síťová opatření	*Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečnosti informací při přenosu musí být počítačové sítě vhodným způsobem spravovány a kontrolovány.*	100
A.10.6.2	Bezpečnost síťových služeb	*Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu.*	100
	Míra plnění daného cíle		100
A.10.7	**Bezpečnost při zacházení s médii**	*Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.*	
A.10.7.1	Správa vyměnitelných počítačových médií	*Musí být vytvořeny postupy pro správu výměnných počítačových médií.*	0

A.10.7.2	Likvidace médií	*Jestliže jsou média dále provozně neupotřebitelná, musí být bezpečně a spolehlivě zlikvidována v souladu se schválenými postupy.*	0
A.10.7.3	Postupy pro manipulaci s informacemi	*Pro zabránění neautorizovanému přístupu nebo zneužití informací musí být stanoveny postupy pro manipulaci s nimi a pro jejich ukládání.*	20
A.10.7.4	Bezpečnost systémové dokumentace	*Systémová dokumentace musí být chráněna proti neoprávněnému přístupu.*	40
	Míra plnění daného cíle		15
A.10.8	**Výměna informací**	*Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.*	
A.10.8.1	Postupy a politiky při výměně informací	*Musí být ustaveny a do praxe zavedeny formální politiky, postupy a opatření na ochranu informací při jejich výměně pro všechny typy komunikačních zařízení.*	20
A.10.8.2	Dohody o výměně informací a programů	*Výměna informací a programového vybavení musí být založena na dohodách uzavřených mezi organizací a externími subjekty.*	20
A.10.8.3	Bezpečnost médií při přepravě	*Média obsahující informace musí být během přepravy mimo organizaci chráněna proti neoprávněnému přístupu, zneužití nebo narušení.*	20
A.10.8.4	Elektronické zasílání zpráv	*Elektronicky přenášené informace musí být vhodným způsobem chráněny.*	20
A.10.8.5	Informační systémy organizace	*Na ochranu informací v propojených podnikových informačních systémech musí být vytvořeny a do praxe zavedeny politiky a postupy*	80
	Míra plnění daného cíle		32
A.10.9	**Služby elektronického obchodu**	*Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití*	
	Míra plnění daného cíle		0
A.10.10	**Monitorování**	*Cíl: Detekovat neoprávněné zpracování informací.*	
A.10.10.1	Pořizování auditních záznamů	*Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, musí být pořizovány a uchovány po stanovené období tak, aby se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu.*	100
A.10.10.2	Monitorování používání systému	*Musí být stanovena pravidla pro monitorování použití prostředků pro zpracování informací, výsledky těchto monitorování musí být pravidelně přezkoumávány.*	20
A.10.10.3	Ochrana vytvořených záznamů	*Prostředky pro zaznamenávání informací a vytvořené záznamy musí být vhodným způsobem chráněny proti zfalšování a neoprávněnému přístupu.*	40
A.10.10.4	Administrátorský a operátorský deník	*Aktivity správce systému a systémového operátora musí být zaznamenávány.*	20
A.10.10.5	Záznam selhání	*Musí být zaznamenány a analyzovány chyby a přijata příslušná opatření.*	20
A.10.10.6	Synchronizace hodin	*Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostní domény synchronizovány se schváleným zdrojem přesného času.*	100
	Míra plnění daného cíle		50

A.11	**Řízení přístupu**		
A.11.1	**Požadavky na řízení přístupu**	*Cíl: Řídit přístup k informacím.*	
A.11.1.1	Politika řízení přístupu	*Musí být vytvořena, zdokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.*	80
	Míra plnění daného cíle		80
A.11.2	**Řízení přístupu uživatelů**	*Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.*	
A.11.2.1	Registrace uživatele	*Musí existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.*	100
A.11.2.2	Řízení privilegovaného přístupu	*Přidělování a používání privilegií musí být omezeno a řízeno.*	100
A.11.2.3	Správa uživatelských hesel	*Přidělování hesel musí být řízeno formálním procesem.*	100
A.11.2.4	Přezkoumání přístupových práv uživatelů	*Vedení organizace musí v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.*	40
	Míra plnění daného cíle		85
A.11.3	**Odpovědnosti uživatelů**	*Cíl: Předcházet neoprávněnému uživatelskému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací.*	
A.11.3.1	Používání hesel	*Při výběru a používání hesel musí být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy.*	100
A.11.3.2	Neobsluhovaná uživatelská zařízení	*Uživatelé musí zajistit přiměřenou ochranu neobsluhovaných zařízení.*	20
A.11.3.3	Zásada prázdného stolu a prázdné obrazovky monitoru	*Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a vyměnitelným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.*	0
	Míra plnění daného cíle		40
A.11.4	**Řízení přístupu k síti**	*Cíl: Předcházet neautorizovanému přístupu k síťovým službám.*	
A.11.4.1	Politika užívání síťových služeb	*Uživatelé musí mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.*	100
A.11.4.2	Autentizace uživatele pro externí připojení	*Přístup vzdálených uživatelů musí být odpovídajícím způsobem autentizován.*	100
A.11.4.3	Identifikace zařízení v sítích	*Pro autentizaci připojení z vybraných lokalit a zařízení musí být zváženo použití automatické identifikace zařízení.*	80
A.11.4.4	Ochrana portů pro vzdálenou diagnostiku a konfiguraci	*Fyzický i logický přístup k diagnostickým a konfiguračním portům musí být řízen.*	100
A.11.4.5	Princip oddělení v sítích	*Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích odděleny.*	20
A.11.4.6	Řízení síťových spojení	*U sdílených sítí, zejména těch, které přesahují hranice organizace, musí být omezeny možnosti připojení uživatelů. Omezení musí být v souladu s politikou řízení přístupu a s požadavky aplikací.*	20

A.11.4.7	Řízení směrování sítě	*Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, musí být zavedeno řízení směrování sítě.*	60
	Míra plnění daného cíle		69
A.11.5	**Řízení přístupu k operačnímu systému**	*Cíl: Předcházet neautorizovanému přístupu k operačním systémům.*	
A.11.5.1	Bezpečné postupy přihlášení	*Přístup k operačnímu systému musí být řízen postupy bezpečného přihlášení.*	100
A.11.5.2	Identifikace a autentizace uživatelů	*Všichni uživatelé musí mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), musí být také zvolen vhodný způsob autentizace k ověření jejich identity.*	100
A.11.5.3	Systém správy hesel	*Systém správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.*	100
A.11.5.4	Použití systémových nástrojů	*Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly, musí být omezeno a přísně kontrolováno.*	100
A.11.5.5	Časové omezení relace	*Neaktivní relace se musí po stanovené době nečinnosti ukončit.*	100
A.11.5.6	Časové omezení spojení	*U vysoce rizikových aplikací musí být pro zajištění dodatečné bezpečnosti použito omezení doby spojení.*	0
	Míra plnění daného cíle		83
A.11.6	**Řízení přístupu k aplikacím a informacím**	*Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.*	
A.11.6.1	Omezení přístupu k informacím	*Uživatelé aplikačních systémů, včetně pracovníků podpory, musí mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu.*	100
A.11.6.2	Oddělení citlivých systémů	*Citlivé aplikační systémy musí mít oddělené (izolované) počítačové prostředí.*	0
	Míra plnění daného cíle		50
A.11.7	**Mobilní výpočetní zařízení a práce na dálku**	*Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku.*	
A.11.7.1	Mobilní výpočetní zařízení a sdělovací technika	*Musí být ustavena formální pravidla a přijata bezpečnostní opatření na ochranu proti rizikům používání mobilních výpočetních a komunikačních zařízení.*	0
A.11.7.2	Práce na dálku	*Organizace musí vytvořit a do praxe zavést zásady, operativní plány a postupy pro práci na dálku.*	80
	Míra plnění daného cíle		40
A.12	**Akvizice, vývoj a údržba informačních systému**		
A.12.1	**Bezpečnostní požadavky informačních systémů**	*Cíl: Zajistit, aby se bezpečnost stala nedílnou součástí informačních systémů.*	
A.12.1.1	Analýza a specifikace bezpečnostních požadavků	*Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů musí obsahovat také požadavky na bezpečnostní opatření.*	0
	Míra plnění daného cíle		0
A.12.2	**Správné zpracování v aplikacích**	*Cíl: Předcházet chybám, ztrátě, neoprávněné modifikaci nebo zneužití informací v aplikacích.*	
A.12.2.1	Validace vstupních dat	*Vstupní data aplikací musí být kontrolována z hlediska správnosti a adekvátnosti.*	100

A.12.2.2	Kontrola vnitřního zpracování	*Pro detekci jakéhokoliv poškození informací vzniklého chybami při zpracování nebo úmyslnými zásahy musí být začleněny kontroly validace dat do aplikace.*	0
A.12.2.3	Integrita zprávy	*U jednotlivých aplikací musí být stanoveny požadavky na zajištění autentizace a integrity zpráv a podle potřeby identifikována a zavedena vhodná opatření.*	0
A.12.2.4	Kontrola výstupních dat	*Pro zajištění toho, že zpracování uložených informací je bezchybné a odpovídající dané situaci, musí být provedeno ověření platnosti výstupních dat z aplikace.*	40
	Míra plnění daného cíle		35
A.12.3	**Kryptografická opatření**	*Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.*	
A.12.3.1	Politika pro použití kryptografických opatření	*Musí být vytvořena a zavedena politika pro používání kryptografických opatření na ochranu informací.*	0
A.12.3.2	Správa klíčů	*Na podporu používání kryptografických technik v organizaci musí existovat systém správy klíčů.*	0
	Míra plnění daného cíle		0
A.12.4	**Bezpečnost systémových souborů**	*Cíl: Zajistit bezpečnost systémových souborů*	
A.12.4.1	Správa provozního programového vybavení	*Musí být zavedeny postupy pro kontrolu instalace programového vybavení na provozních systémech.*	100
A.12.4.2	Ochrana systémových testovacích údajů	*Testovací data musí být pečlivě vybrána, chráněna a kontrolována.*	80
A.12.4.3	Řízení přístupu ke knihovně zdrojových kódů	*Přístup ke knihovně zdrojových kódů musí být omezen.*	40
	Míra plnění daného cíle		73
A.12.5	**Bezpečnost procesů vývoje a podpory**	*Cíl: Udržovat bezpečnost programového vybavení a informací aplikačních systémů.*	
A.12.5.1	Postupy řízení změn	*Musí být zavedeny formální postupy řízení změn.*	80
A.12.5.2	Technické přezkoumání aplikací po změnách operačního systému	*V případě změny operačního systému musí být přezkoumány a otestovány kritické aplikace, aby bylo zajištěno, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.*	20
A.12.5.3	Omezení změn programových balíků	*Modifikace programových balíků musí být omezeny pouze na nezbytné změny, veškeré prováděné změny musí být řízeny.*	80
A.12.5.4	Unik informací	*Musí být zabráněno příležitostem k úniku informací.*	0
A.12.5.5	Programové vybavení vyvíjené externím dodavatelem	*Organizace musí dohlížet a monitorovat vývoj programového vybavení externím dodavatelem.*	0
	Míra plnění daného cíle		36
A.12.6	**Řízení technických zranitelností**	*Cíl: Snížit rizika vyplývající z využívání zveřejněných technických zranitelností.*	
A.12.6.1	Řízení, správa a kontrola technických zranitelností	*Musí být zajištěno včasné získání informací o existenci technických zranitelností v provozovaném informačním systému, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na pokrytí souvisejících rizik.*	60
	Míra plnění daného cíle		60

A.13	**Zvládání bezpečnostních incidentů**		
A.13.1	**Hlášení bezpečnostních událostí a slabin**	*Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.*	
A.13.1.1	Hlášení bezpečnostních událostí	*Bezpečnostní události musí být co nejrychleji hlášeny příslušnými řídícími kanály.*	0
A.13.1.2	Hlášení bezpečnostních slabin	*Všichni zaměstnanci, smluvní strany a ostatní uživatelé informačního systému a služeb musí být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.*	0
	Míra plnění daného cíle		0
A.13.2	**Zvládání bezpečnostních incidentů a kroky k nápravě**	*Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.*	
A.13.2.1	Odpovědnosti a postupy	*Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty musí být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.*	0
A.13.2.2	Ponaučení z bezpečnostních incidentů	*Musí existovat mechanizmy, které by umožňovaly kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů.*	0
A.13.2.3	Shromaždování důkazů	*V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (podle práva občanského nebo trestního) vůči osobě anebo organizaci, musí být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat.*	0
	Míra plnění daného cíle		0
A.14	**Řízení kontinuity činností organizace**		
A.14.1	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**	*Cíl: Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činností.*	
A.14.1.1	Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace	*V rámci organizace musí existovat řízený proces pro rozvoj a udržování kontinuity činností organizace.*	0
A.14.1.2	Kontinuita činností organizace a hodnocení rizik	*Musí být identifikovány možné příčiny přerušení činností organizace, včetně jejich pravděpodobnosti, velikosti dopadu a možných následků na bezpečnost informací.*	0
A.14.1.3	Vytváření a implementace plánů kontinuity	*Pro udržení nebo obnovení provozních činností organizace po přerušení nebo selhání kritických procesů a pro zajištění dostupnosti informací v požadovaném čase a na požadovanou úroveň musí být vytvořeny a implementovány plány.*	0
A.14.1.4	Systém plánování kontinuity činností organizace	*Pro zajištění konzistence plánů kontinuity činností a pro určení priorit testování a údržby musí být k dispozici jednotný systém plánů kontinuity činností organizace.*	0
A.14.1.5	Testování, udržování a přezkoumání plánů kontinuity	*Plány kontinuity činností organizace musí být pravidelně testovány a aktualizovány, aby se zajistila jejich aktuálnost a efektivnost.*	0
	Míra plnění daného cíle		0

A.15	**Soulad s požadavky**		
A.15.1	**Soulad s právními normami**	*Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.*	
A.15.1.1	Identifikace odpovídajících předpisů	*Pro každý informační systém musí být jednoznačně definovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, regulatorní a smluvní požadavky a způsob, jakým je organizace dodržuje.*	100
A.15.1.2	Ochrana duševního vlastnictví	*Pro zajištění souladu se zákonnými, regulatorními a smluvními požadavky na použití materiálů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví, musí být zavedeny vhodné postupy.*	0
A.15.1.3	Ochrana záznamů organizace	*Důležité záznamy organizace musí být chráněny proti ztrátě, zničení a padělání a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.*	0
A.15.1.4	Ochrana dat a osobních údajů	*Ochrana dat a soukromí musí být zajištěna v souladu s odpovídající legislativou, předpisy, a pokud je to relevantní, se smlouvami.*	100
A.15.1.5	Prevence zneužití prostředků pro zpracování informací	*Musí být zakázáno používat prostředky pro zpracování informací jiným než autorizovaným způsobem.*	60
A.15.1.6	Regulace kryptografických opatření	*Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, zákony a předpisy.*	0
	Míra plnění daného cíle		43
A.15.2	**Soulad s bezpečnostními politikami, normami a technická shoda**	*Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.*	
A.15.2.1	Shoda s bezpečnostními politikami a normami	*Vedoucí zaměstnanci musí zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami.*	60
A.15.2.2	Kontrola technické shody	*Informační systémy musí být pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy.*	0
	Míra plnění daného cíle		30
A.15.3	**Hlediska auditu informačních systémů**	*Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do/z informačních systémů.*	
A.15.3.1	Opatření k auditu informačních systémů	*Požadavky auditu a činnosti zahrnující kontrolu provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace.*	0
A.15.3.2	Ochrana nástrojů pro audit informačních systémů	*Přístup k nástrojům určeným pro audit informačních systémů musí být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.*	0
	Míra plnění daného cíle		0
	Míra plnění ISMS		**44,6**